BOLETÍN OFICIAL
DE LAS CORTES GENERALES

CONGRESO DE LOS DIPUTADOS

XIV LEGISLATURA

Serie B:
PROPOSICIONES DE LEY **26 de julio de 2021** **Núm. 173-1** **Pág. 1**

PROPOSICIÓN DE LEY

122/000148 Proposición de Ley para la Transformación Digital de España.

Presentada por el Grupo Parlamentario Popular en el Congreso.

La Mesa de la Cámara, en su reunión del día de hoy, ha adoptado el acuerdo que se indica respecto del asunto de referencia.

(122) Proposición de ley de Grupos Parlamentarios del Congreso.

Autor: Grupo Parlamentario Popular en el Congreso.

Proposición de Ley para la Transformación Digital de España.

Acuerdo:

Admitir a trámite, trasladar al Gobierno a los efectos del artículo 126 del Reglamento, publicar en el Boletín Oficial de las Cortes Generales y notificar al autor de la iniciativa.

En ejecución de dicho acuerdo se ordena la publicación de conformidad con el artículo 97 del Reglamento de la Cámara.

Palacio del Congreso de los Diputados, 20 de julio de 2021.—P.D. El Secretario General del Congreso de los Diputados, **Carlos Gutiérrez Vicén.**

A la Mesa del Congreso de los Diputados

El Grupo Parlamentario Popular en el Congreso, al amparo de lo establecido en el artículo 124 y siguientes del vigente Reglamento de la Cámara, formula la siguiente Proposición de Ley para la Transformación Digital de España.

Palacio del Congreso de los Diputados, 22 de junio de 2021.—**Concepción Gamarra Ruiz-Clavijo,** Portavoz del Grupo Parlamentario Popular en el Congreso.

cve: BOCG-14-B-173-1

PROPOSICIÓN DE LEY PARA LA TRANSFORMACIÓN DIGITAL DE ESPAÑA

Exposición de motivos

I

Se denomina Cuarta Revolución Industrial a la transformación tecnológica producida desde los años 80 del siglo XX y que afecta no sólo a la producción industrial sino también a múltiples aspectos de nuestra vida cotidiana. Pero esta revolución no se caracteriza sólo por el descubrimiento de un conjunto de tecnologías emergentes, sino por iniciar un proceso de transición hacia nuevos sistemas sustentados en la digitalización. Las nuevas tecnologías, denominadas tecnologías disruptivas, han cambiado la tradicional forma de trabajar, comprar o relacionarse de las personas. La revolución digital ofrece ahora una oportunidad de crecimiento en todos los sectores económicos y sociales, pero éstos precisan de una verdadera transformación para integrarla en sus procesos y generar el beneficio productivo, social y medioambiental que exige la nueva economía. La transformación digital supone la integración de las nuevas tecnologías en todas las áreas de la sociedad para optimizar los resultados, mejorar la competitividad de las empresas y ofrecer un nuevo valor añadido a la ciudadanía en sus relaciones económicas, sociales, educativas, sanitarias y con la administración. La digitalización ofrece un enorme potencial para ganar competitividad en un mundo cada vez más tecnológico, pero contempla también aspectos relativos a la seguridad de los países y al ámbito de la ética. Así pues, el nuevo escenario digital necesita una normativa que lo desarrolle, impulse, proteja y respalde. En la actualidad, la Cuarta Revolución Industrial o Industria 4.0 está llamada a introducir importantes cambios económicos y sociales y a exigir una transformación en la estructura, formación y reglas de juego del mundo empresarial.

La revolución digital se basa en el desarrollo de las comunicaciones electrónicas, nanotecnología, neurotecnología, robots, inteligencia artificial, biotecnología, sistemas de almacenamiento de energía, drones, impresoras 3D o computación en la nube, lo que deriva en multitud de aplicaciones cuyo uso debe ser regulado y especialmente incentivado. Avances como Internet de las Cosas (IoT), *Big Data, Blockchain* o 5G forman parte de un ecosistema que está cambiando la forma de vivir y trabajar de las personas. La aceleración de la digitalización y la reducción de los costes generan nuevas necesidades de innovación, no sólo en el sector público sino también en el ámbito privado y personal. Las empresas españolas se enfrentan al reto de la digitalización, para poder competir en un mundo productivo cada vez más tecnológico y global, y necesitan la ayuda de las administraciones públicas. Como sucedió en otras etapas de la historia económica, esta nueva realidad requiere con urgencia una normativa que se adapte a los cambios sociales y económicos que derivan de la Revolución Digital que se desarrolla en todos los ámbitos de la vida y cuyo crecimiento es ya imparable.

II

En julio de 2020, el Gobierno presentó la nueva Agenda Digital, con el nombre de España Digital 2025. La Orden ETD/920/2020, de 28 de septiembre, por la que se crea y regula el Consejo Consultivo para la Transformación Digital, es una concreción de dicho Plan y se desarrolla en la Resolución de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (BOE-A-2020-13673) de 3 de noviembre, por la que se determina la composición de la Comisión Permanente de Telecomunicaciones, Infraestructuras Digitales, Conectividad Digital y Sector Audiovisual, creada en el seno del Consejo Consultivo para la Transformación Digital. Pero este plan debe concretarse en una legislación que respalde la transformación digital de la sociedad española. La nueva economía digital necesita, ahora, un período de transición que tenga como objetivo sentar las bases legales de una sociedad digital sostenible que genere confianza en el futuro, garantice la competitividad del tejido productivo y mitigue los impactos negativos transitorios.

III

La digitalización de las Administraciones Públicas debe realizarse, de forma urgente, para garantizar a los ciudadanos españoles sus derechos digitales, protegerlos de los ciberataques, facilitarles el acceso a las nuevas tecnologías, eliminar la brecha digital y poner a su disposición unos servicios públicos más ágiles y eficientes, sin olvidar la necesaria protección del menor en su relación con las herramientas

cve: BOCG-14-B-173-1

digitales. Así pues, los cambios tecnológicos que impulsan la innovación en el sector privado deben ir acompañados de una respuesta, también digital, de las Administraciones Públicas que están obligadas a resolver con eficacia los trámites burocráticos que exige la ciudadanía. El artículo 14 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece que los poderes públicos reconocen el derecho y la obligación de relacionarse electrónicamente con las Administraciones Públicas y el compromiso de adoptar las medidas que posibiliten dicho derecho y obligación. El artículo 2.b) de la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que la Comisión Sectorial de la administración electrónica tiene, entre sus funciones, impulsar el desarrollo de la administración electrónica en España. En el Real Decreto-ley 14/2019, de 31 de octubre, se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones y, finalmente, el Real Decreto-ley 28/2020, de 22 de septiembre, regula el trabajo a distancia. Corresponde al Gobierno modernizar el sistema administrativo y la política de recursos humanos, que debe incluir la formación digital.

IV

Las pequeñas y medianas empresas (PYME) constituyen el 99,8 % del tejido empresarial español. La pandemia ha puesto de manifiesto que muchas de ellas sufren un retraso tecnológico, lo que implica la urgencia de adaptarse al actual contexto cambiante. La planificación de recursos, la previsión y las cuentas, la gestión de la cadena de suministro o la contabilidad han sido las funciones más digitalizadas antes de la COVID-19. Las empresas se ven obligadas a digitalizar las inversiones de nuevos procesos de venta, la gestión de la fuerza laboral, la publicidad o el servicio al cliente.

Especial atención, por su alta generación de valor y su potencial de crecimiento a corto plazo, merecen las PYMEs con productos innovadores y disruptivos, denominadas *Startups,* fuertemente orientadas al cliente y con un uso intensivo de las tecnologías de la información y las comunicaciones. España asiste a un rápido crecimiento de las *startups* tecnológicas. En todas las Comunidades Autónomas surgen iniciativas de emprendimiento e innovación que necesitan urgentemente el apoyo de la Administración Pública, mediante incentivos fiscales y la simplificación de los procedimientos burocráticos. En España, las diversas leyes, en especial las mercantiles y tributarias, no tienen en cuenta las particularidades de estos nuevos modelos de negocio: Ley 11/2013, de 26 de julio, de medidas de apoyo al emprendedor y de estímulo del crecimiento y de la creación de empleo; Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización; Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad; y Ley 5/2015, de 27 de abril, de Fomento de la Financiación Empresarial que regula el micromecenazgo *(crowdfunding, en inglés).* En este sentido, los fondos de capital privado, en operaciones de *Prívate Equity y Venture Capital* deben contribuir a la reconstrucción económica de nuestro país, asegurando el mantenimiento e impulso de las empresas, como pilar fundamental para el desarrollo del tejido empresarial basado en las *startups* tecnológicas e innovadoras. Por ello, se hace necesario adaptar el marco normativo español al de los países de nuestro entorno para fomentar la inversión y facilitar la financiación privada de las empresas españolas que lo necesiten.

V

Se denomina *Sandbox* a un espacio donde las empresas pueden probar sus nuevos productos, servicios, y modelos de negocio de una forma segura, sin tener que atenerse a toda la regulación que, en circunstancias normales, requeriría dicha actividad y bajo condiciones de supervisión. El Congreso de los Diputados aprobó el 18 de febrero de 2020 el Proyecto de Ley para la Transformación Digital del Sistema Financiero, que permite llevar a la práctica proyectos tecnológicos de innovación en este ámbito. Es el momento de ampliar la normativa a todos aquellos sectores que presenten nuevos modelos de negocio basados en ideas o tecnologías disruptivas, de manera que puedan ser testados y validados sin colisionar con la regulación existente. Es necesaria una nueva legislación de *sandbox* que permita desarrollarse a empresas de otros sectores como farmacia, atención primaria, logística, postal, seguridad, energía, seguridad vial o movilidad.

cve: BOCG-14-B-173-1

VI

El sector de las telecomunicaciones se encuentra en un momento crucial que requiere acometer fuertes niveles de inversión en despliegues de nuevas infraestructuras de comunicaciones fijas, radiocomunicaciones o inalámbricas, en un momento en que los retornos de dichas inversiones presentan incertidumbre, especialmente motivada por la crisis generada por COVID-19. A esta situación, se suma un problema creciente de fiscalidad que supone una importante desmotivación para el despliegue e inversión en infraestructuras de los operadores de comunicaciones electrónicas tradicionales. La presión fiscal del sector de las telecomunicaciones es muy elevada, superior a la que recae en otros sectores de actividad en España y Europa, ya que los operadores suman tributos estatales, autonómicos, locales y otros específicos del sector que afectan directamente a su capacidad inversora y, por tanto, al desarrollo digital de nuestro país. España no sólo posee los tipos más elevados en la mayoría de los conceptos impositivos, sino que además contempla un mayor número de figuras tributarias. Por tanto, la presente regulación debe servir para abordar este problema de fiscalidad, teniendo en cuenta que la transformación digital de España depende de la conectividad y el despliegue de las redes de nueva generación.

VII

La Industria Digital y la Inteligencia Artificial son dos conceptos que evidencian un cambio radical en la forma de producción a gran escala y la fabricación de todo tipo de bienes industriales y productos cotidianos. La Inteligencia Artificial (IA), aporta beneficios importantes a la industria como la mejora de los procesos y servicios, la reducción de los costes, el uso eficaz de los recursos, la predicción de comportamientos futuros o la corrección de los errores de producción actual, ofreciendo mayor calidad, rapidez y eficiencia, tal y como demanda la sociedad. Las principales plataformas digitales ofrecen ya la IA como uno de sus servicios debido a la necesidad de gestionar la enorme cantidad de datos que manejan, empleando algoritmos predictivos que ofrecen al usuario recomendaciones basadas en su historial de búsquedas o compras e, incluso, predicen las decisiones de búsqueda del usuario en Internet. La proliferación de datos, la progresiva capacidad tecnológica para automatizar procesos y la aparición de técnicas basadas en el aprendizaje de máquinas han permitido que la IA esté siendo ya aplicada a múltiples sectores. En el año 2017, la comisión de Asuntos Jurídicos del Parlamento Europeo instó a la Unión Europea (UE) a armonizar las normas de seguridad, éticas y legales para regular los importantes progresos en el campo de la robótica y de la Inteligencia Artificial. El Consejo Europeo celebrado en octubre de 2017 señaló que la UE necesita concienciarse de la urgencia de hacer frente a las nuevas tendencias, tales como la IA, garantizando también un elevado nivel de protección de los datos, los derechos digitales y las normas éticas, mediante un planteamiento europeo común a esta tecnología. El retraso en Europa respecto al desarrollo de la IA precisa de actuaciones regulatorias en España para crear un entorno que propicie las inversiones y que haga uso de la financiación pública para estimular las inversiones privadas. Así pues, el marco ofrecido por la Directiva 85/374/CEE no es suficiente para aprovechar las capacidades de la nueva generación de robots, en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento, convirtiéndolos en robots inteligentes. Tanto los ciudadanos como las empresas deben poder confiar en la tecnología con la que interactúan, disponer de un entorno jurídico predecible y contar con la garantía efectiva de la protección de los derechos y libertades fundamentales. Para aumentar la transparencia y reducir el riesgo de sesgo o error, los sistemas de IA deben desarrollarse de tal modo que las personas puedan comprender cuál es la base de sus acciones. En marzo de 2019, la Comisión Europea redactó un informe para abordar las cuestiones éticas que plantea la tecnología inteligente, poniendo el énfasis en la supervisión humana y el foco en el bienestar social, en la diversidad y en el respeto medioambiental como último fin de la IA. El 19 de febrero de 2020, la Comisión Europea publicó el Libro Blanco de la Inteligencia Artificial, con el objetivo de poner en marcha una amplia consulta de la sociedad civil, la industria y el mundo académico de los Estados, con propuestas concretas en torno a un enfoque europeo.

Muchas aplicaciones basadas en IA, tienen una gran repercusión en el derecho a la intimidad de las personas. El reconocimiento facial y biométrico es un ámbito clave en el que la IA puede afectar a los derechos fundamentales. Su uso con fines de identificación personal está sujeto al Reglamento General de Protección de Datos —Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016—, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

cve: BOCG-14-B-173-1

personales, a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE) y al artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Sin embargo, no existe límite en el uso generalizado del reconocimiento biométrico basado en IA para otras actuaciones de clasificación en función de comportamientos o emociones de los seres humanos.

VIII

Big Data es una tecnología que permite a empresas y administraciones dirigir sus actividades y servicios hacia un mercado o hacia usuarios, extraídos del análisis de millones de datos de distintas fuentes, de manera que sea posible tomar decisiones comerciales de forma rápida y precisa. Y cada vez tiene más efectividad, porque el avance de la tecnología permite que los costes de almacenaje de datos sean más económicos. Esta tecnología, bien empleada, tiene la capacidad de mejorar la gestión del medio ambiente, la salud, la productividad o la vida personal. Así pues, la tecnología *Big Data y* su ecosistema proporcionan el procesamiento y análisis de una gran cantidad de datos que aportan los negocios y las grandes empresas, pero que necesita mejorar en integridad, seguridad y transparencia. Por tanto, el dato y sus sistemas de almacenamiento y computación se han convertido en una infraestructura clave que hay que proteger y desarrollar en el territorio español, habida cuenta de lo relevante y crítico que puede resultar para el actual y futuro uso en la práctica totalidad de sectores productivos. Por otro lado, es necesario establecer un marco jurídico que potencie esta tecnología, bajo el cumplimiento de las leyes de protección a consumidores e inversores, el establecimiento de unos requisitos reforzados para compradores no cualificados, la transparencia y la estabilidad financiera del sistema. La Unión Europea promulgó el Reglamento 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuyo objetivo es que los ciudadanos puedan controlar y decidir sobre el uso de sus datos. En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD) derogó a la anterior Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. En esta Ley se establecen las bases regulatorias para la adaptación de esta tecnología a las nuevas realidades de una economía digital.

IX

La computación en la nube *(cloud computing,* en inglés) es una tecnología que permite una mayor eficiencia en el uso de los recursos naturales con el consecuente beneficio para el medio ambiente y que consiste en el acceso remoto, desde cualquier lugar del mundo y en cualquier momento, a *software,* almacenamiento de archivos y procesamiento de datos a través de Internet, sin la necesidad de conectarse a un ordenador personal o servidor local. Al mismo tiempo, permite al usuario acceder a recursos, programas e información desde cualquier dispositivo electrónico en ubicaciones de dichos datos que pueden no ser conocidas por el usuario. La tecnología *Cloud* es uno de los mayores avances tecnológicos y socioeconómicos de los últimos 20 años como elemento habilitador y democratizador del acceso a la innovación y a las tecnologías de la información más avanzadas, ya que facilita a todas las personas el acceso a las últimas tecnologías a precios muy bajos. Mediante esta tecnología, cualquier empresa o administración pública, desde el más pequeño de los ayuntamientos con un presupuesto muy limitado hasta el mayor de los ministerios u organismos internacionales, pueden tener acceso al mismo catálogo de productos y servicios tecnológicos. Con el objeto de favorecer el desarrollo de centros de computación y acceso a contratación por parte de las empresas, es necesario establecer programas de apoyo y colaboración público-privada para la implantación de centros *Cloud,* así como su consideración como industria electrointensiva, según el Estatuto publicado en el Real Decreto 1106/2020, de 15 de diciembre.

X

Los avances científicos y técnicos han contribuido en los últimos años a la progresiva reducción del coste del sector industrial de las aeronaves no tripuladas pilotadas por control remoto o autónomos, denominadas comúnmente drones, que son vehículos aéreos no tripulados. El artículo 50 de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad

cve: BOCG-14-B-173-1

y la eficiencia, realiza ciertas modificaciones sobre legislación aérea, con la aclaración de que las aeronaves no tripuladas pilotadas por control remoto son efectivamente aeronaves y, como tales, su utilización civil está sujeta a la legislación aeronáutica. El Real Decreto 1036/2017, de 15 de diciembre, regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifica el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, el que supuso un gran avance en la normativa existente y un paso importante para el establecimiento de un marco jurídico definitivo aplicable a la utilización civil de estas aeronaves no tripuladas, no sujetas a la normativa de la Unión Europea. El citado real decreto prevé también la posibilidad de realizar operaciones aéreas especializadas en distintos ámbitos, a través del cumplimiento de una serie de requisitos, el desarrollo de estudios aeronáuticos de seguridad correspondientes o la solicitud del permiso a la Agencia Española de Seguridad Aérea. La Comisión Europea ha regulado, mediante reglamentos, algunos aspectos sobre el uso de las aeronaves no tripuladas (Reglamento 2018/1139, 2019/945 y 2019/947). Así pues, en España es necesario regular ahora el desarrollo de aerovías que permitan a los drones circular por un espacio aéreo exclusivo, lo que favorecerá el desarrollo de nuevos servicios logísticos en aquellos casos en los que estas aeronaves pudieran ser utilizadas para realizar transporte de pequeñas mercancías o materiales, hecho que favorecerá especialmente a los habitantes de las zonas rurales en situación de aislamiento o confinamiento.

XI

Los vehículos terrestres son, cada vez, más complejos desde el punto de vista tecnológico. La informatización de los vehículos permite la conexión con otros dispositivos, dando lugar al concepto de «coche conectado» que la Sociedad de Tecnología Vehicular (VTS, por sus siglas en inglés) define como aquél que equipa aplicaciones, servicios y tecnologías que lo conectan con su entorno. La incorporación al vehículo del Sistema Avanzado de Apoyo a la Conducción (ADAS, por sus siglas en inglés), según diversos estudios, pueden reducir los gastos por siniestralidad o accidentes de tráfico en 4.500 millones de euros y evitar 25.000 muertes y 140.000 heridos graves, hasta el año 2038 en Europa.

La Unión Europea ha aprobado el Reglamento (UE) 2019/2144 del Parlamento Europeo y del Consejo, de 27 de noviembre, relativo a los requisitos de homologación de tipo de los vehículos de motor y de sus remolques, así como de los sistemas, componentes y unidades técnicas independientes destinadas a esos vehículos, en lo que respecta a su seguridad general y a la protección de los ocupantes y de los usuarios vulnerables de la vía pública. Esto implica la incorporación obligatoria de un paquete de diez sistemas de seguridad en todos los nuevos modelos de turismos y furgonetas ligeras que se vendan en el mercado a partir de 2022, así como todos los nuevos modelos fabricados a partir de 2024. De esta manera, los vehículos deberán incorporar o preinstalar algunos sistemas como pueden ser: frenado autónomo de emergencia urbano e interurbano; alerta de tráfico cruzado; detector de somnolencia y sistemas de reconocimiento y prevención de distracciones; sistema de detección de peatones; sistema de cambio involuntario de carril; detección o avisador de ángulo muerto; control de crucero adaptativo para vigilar la distancia entre vehículos en carretera; limitador de velocidad con reconocimiento de señales, bloqueo del vehículo con alcoholímetro o caja negra.

En enero de 2017, la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA, por sus siglas en inglés) publicó un estudio centrado en la seguridad cibernética y la resistencia de los automóviles inteligentes que enumera los activos sensibles, así como las correspondientes amenazas, riesgos, factores de mitigación y posibles medidas de seguridad. Sin embargo, el marco legal aplicable a los coches conectados de la UE es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que se aplica cuando el procesamiento de datos implica el manejo datos personales. En España, los usuarios de un vehículo conectado están protegidos por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Es preciso impulsar ahora nuevas medidas para incrementar aún más la ciberseguridad de estos vehículos a medida que avanza su desarrollo e implementación que permita el impulso de esta tecnología con las mayores garantías.

Más de 50 países, entre ellos España, junto con los miembros de la Unión Europea, han firmado en la Organización de Naciones Unidas el reglamento para la prevención de la ciberseguridad (VVP29/2020/79)

cve: BOCG-14-B-173-1

que afecta a coches, autobuses, camiones, auto caravanas y remolques. Esta normativa exigirá un certificado de ciberseguridad a todos los vehículos que sean homologados a partir del 1 de enero de 2022. Además, en 2024, ningún vehículo nuevo podrá comercializarse sin atenerse a sus criterios. Esto significa que fabricantes y suministradores de componentes tienen poco tiempo para adaptarse a las estrictas nuevas exigencias legales y España no puede ser ajena a ello.

XII

El Internet de las cosas (IoT, por sus siglas en inglés) es un concepto que se refiere a una interconexión de todo tipo de sensores y de objetos cotidianos a través de internet. A finales de 2019 existían 9.500 millones de dispositivos IoT conectados en el mundo, sin contar con teléfonos móviles y ordenadores. En los próximos años, la demanda incrementará esta cifra hasta 28.000 millones en 2024 y 40.000 millones en 2027. La tecnología IoT está ya en todos los ámbitos: salud, agricultura y ganadería, movilidad, ciudades, hogar, comercio e incluso hasta en la ropa y complementos como chaquetas, calzado, relojes, pulseras, gafas, etc. Por este motivo, debe elaborarse una legislación que obligue a las empresas a establecer unos requisitos de seguridad para los dispositivos capaces de conectarse a Internet, directa o indirectamente, y que tengan asignada una dirección de Protocolo de Internet, una dirección *Bluetooth* o cualquier otro tipo de red inalámbrica o satelital, fomentando el desarrollo de esta tecnología.

XIII

En el año 2009, se puso en marcha la tecnología *Blockchain* a través de la primera moneda virtual descentralizada, el *bitcoin,* que consigue evitar intermediarios que validen los intercambios de esta moneda. Es la propia tecnología la que garantiza que la información sea correcta y esté sincronizada entre los participantes de la red. *Blockchain* es similar a un libro de registro inmodificable y compartido para registrar el historial de transacciones, estableciendo altos niveles de confianza, responsabilidad y transparencia para cualquier activo, además de los pagos o escrituras. En Sentencia de octubre de 2015 (asunto C-264/14, apartado 24) el Tribunal de Justicia Europea (TJUE) decretó que el *bitcoin* es una «divisa virtual de flujo bidireccional» que se intercambia por divisas internacionales en las operaciones de cambio de moneda y que «no puede calificarse de bien corporal» porque su única finalidad es la de ser «un medio de pago». A través de las diferentes tecnologías *Bockchain,* se puede lograr la certificación inmutable de información, la representación de valor (cualquier activo físico o digital) como dinero, productos financieros, propiedad intelectual o contratos. Al actuar la tecnología *Blockchain* como una fuente de confianza entre las partes, tiene el potencial de transformar el papel de muchos intermediarios como se conocen hoy en día, siempre y cuando la regulación se adapte y lo permita. Por otra parte, en el mundo financiero virtual han surgido las denominadas ICO *(Initial Coin Offering* u oferta inicial de moneda), como metodología de financiación de proyectos mediante la venta de tokens —ficha que puede ser una criptomoneda emitida por la propia empresa, una participación en acciones o un derecho a recibir un producto o servicio— por medio de la tecnología *Blockchain.* Se perfila como una herramienta innovadora y exitosa para captación de inversión por parte de nuevas empresas *(startups)* y la circulación de nuevas divisas virtuales. Recientes casos de fraude, estafas y ataques de hackers relacionados con las ICO han activado acciones por parte de las autoridades de diversos países y han puesto en evidencia la necesidad de una legislación, dando origen a la publicación de la Directiva 2018/843/UE, del Parlamento Europeo y del Consejo, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE. La Resolución de 8 de enero de 2018, de la Dirección General de la Agencia Estatal de Administración Tributaria (AET), aprueba las directrices generales del Plan Anual de Control Tributario y Aduanero de 2018, en el que se establece la vigilancia, por parte de la AEAT, del uso de las criptomonedas. En el caso de España, existe una regulación fragmentaria para cada sector por lo que es necesaria una legislación armonizada que proteja al inversor.

XIV

El Real Decreto-Ley 15/1977 de 25 de febrero, sobre medidas fiscales, financieras y de inversión pública, establece la adopción de medidas concretas directamente encaminadas a resolver los problemas

cve: BOCG-14-B-173-1

planteados por la realidad de la coyuntura económica actual. El artículo 35 y 39 del Capítulo IV de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, regula los incentivos aplicables a los ejercicios fiscales y concreta las medidas de apoyo a las empresas y a sus normas de aplicación. Es urgente apoyar a la empresa española en su proceso de digitalización y a los empresarios a diseñar su propio plan de desarrollo para su empresa en el ámbito de la innovación y la digitalización. Para ello, esta ley establece los incentivos fiscales para que las empresas tecnológicas, o que utilicen tecnología digital en sus procesos, puedan situarse al mismo nivel que el de los países más avanzados.

XV

La defensa del medio ambiente es una tarea siempre pendiente. España debe comprometerse a la eliminación de los residuos contaminantes que ponen en peligro la salud de las personas. En este sentido, es importante legislar sobre la obsolescencia programada que consiste en la determinación del fin de la vida útil de un producto, en especial del ámbito digital tecnológico, de modo que tras un período de tiempo calculado previamente por el fabricante se vuelve obsoleto e inservible por falta de repuestos o dificultad de reparación, evitando el lucro económico de las empresas a través de la generación de compras más frecuentes para reemplazar el producto dañado y crear una relación de fidelización por la que se obtienen beneficios económicos a largo plazo. Esta práctica provoca, además, una serie de problemas colaterales de tipo medioambiental como el agotamiento de los recursos y la generación de residuos contaminantes. España debe ahora regular la práctica de la obsolescencia programada en los productos digitales en el ámbito de la economía circular que implica compartir, alquilar, reutilizar, reparar, renovar y reciclar materiales y productos existentes todas las veces que sea posible, con el fin de crear valor añadido.

XVI

Es probable que los trabajos menos cualificados sean más vulnerables a la automatización, por lo que, parece fundamental su reciclaje hacia otras capacidades profesionales. Los nuevos desarrollos tecnológicos y la hiperconectividad, plantean retos y oportunidades históricas para el desarrollo de la industria inteligente española. Además, la transformación digital ha contribuido a dar solución a muchos de los problemas derivados del confinamiento de la población a causa de la pandemia del coronavirus, lo que exige un cambio en cuanto a su organización y formación que permita afrontar una circunstancia de estas características, promoviendo el teletrabajo y la enseñanza virtual. Para ello, se ha publicado el Real Decreto-ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud con el fin de hacer frente a la crisis sanitaria ocasionada por la COVID-19. Pero este cambio en la forma de trabajar, de estudiar o de enseñar, ha dejado al descubierto la necesidad de formar a trabajadores, profesorado y alumnado en unas competencias digitales que deben ser reguladas e impulsadas.

Por otro lado, la competencia digital va a resultar clave para la formación a lo largo de la vida; comprende un conjunto de conocimientos, habilidades, actitudes y estrategias que se requieren para el uso de los medios digitales y de las tecnologías de la información y la comunicación. La formación en habilidades digitales es fundamental para el fortalecimiento de las empresas y sus modelos de negocio, lo que requiere que los planes educativos escolares, de formación profesional y universidades, en el ámbito de sus competencias, se adecuen a la nueva realidad digital.

XVII

El ciberespacio debe protegerse como parte de nuestra soberanía. Un ciberataque a una institución pública, organización o empresa puede dañar la confidencialidad, integridad y disponibilidad de la información, afectando gravemente a los intereses de la entidad, clientes u otros organismos relacionados. Los países del entorno de la Unión Europea, en el marco de una política de ciberdefensa común, están adaptando sus normativas para la protección de sus respectivas naciones y crear estructuras de conocimiento y recursos que puedan ser activados en caso de graves amenazas contra las infraestructuras de un país. El artículo 122 de la Ley 39/2007, de 19 de noviembre, de la carrera militar, indica que las Fuerzas Armadas cuentan con un número de efectivos a los cuales se pueden sumar los reservistas, definidos como aquellos españoles que, en aplicación del derecho y deber constitucionales de defender a

cve: BOCG-14-B-173-1

España, pueden ser llamados a incorporarse a las Fuerzas Armada para participar en las misiones definidas en la Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional. Por todo ello, y tal como recoge la Ley 39/2007, existe una necesidad urgente de contar con una Reserva Estratégica en materia de ciberdefensa para combatir las amenazas exteriores a nuestro país y a cualquier miembro de la Unión Europea. El papel de los reservistas cibernéticos puede ser de vital importancia para la defensa de las plataformas digitales de instituciones y particulares en tiempo de pandemia y otras situaciones excepcionales o críticas. Por todo ello, es de especial interés la creación de una Reserva Estratégica de Talento en Ciberseguridad formada por reservistas voluntarios que actuarían, tal y como especifica el artículo 123 de la Ley 39/2007, de 19 de noviembre, de la carrera militar, si las necesidades de la defensa nacional no pudieran ser atendidas por los efectivos de militares profesionales, en apoyo de las necesidades dentro del ámbito específico de la ciberdefensa.

XVIII

La presente ley consta de seis títulos, que se disponen en sesenta y un artículos, cuatro disposiciones adicionales, una disposición derogatoria y tres disposiciones finales.

El Título Preliminar, «Ámbito de aplicación y los principios generales», comprende cinco artículos: el artículo uno establece el objeto de la ley, que consiste en elaborar el ámbito legislativo para facilitar el proceso de transición de la industria española hacia la industria digital en todos sus ámbitos; el artículo dos indica el ámbito de aplicación; el artículo tres señala el ámbito territorial; el artículo cuatro define los principios de la ley en el sector público, en el sector privado y en el ámbito de los ciudadanos; y el artículo cinco expone las definiciones de los conceptos específicos que aparecen en la ley.

El Título Primero, «Gobernanza de la Transformación Digital en España», contiene cuatro artículos: el artículo seis trata de la Administración Pública Digital; el artículo siete crea la Oficina Técnica para la Financiación Digital; el artículo ocho establece la gobernanza para la digitalización; y el artículo nueve regula el Consejo Consultivo para la Transformación Digital.

El Título Segundo, «Competitividad y competencias digitales», contempla ocho artículos: el artículo diez recoge las actuaciones para la digitalización de las PYMES a través de un Plan de Digitalización; el artículo once incluye medidas sobre financiación; el artículo doce establece medidas sobre fiscalidad en el ámbito digital; el artículo trece menciona las acciones de responsabilidad social de las empresas para gestionar el impacto de la actividad digital en el entorno laboral, medioambiental y social; el artículo catorce establece las medidas para obtener las competencias digitales demandadas por el proceso de transformación digital; el artículo quince trata las actuaciones para incentivar la creación de *startups* de tecnologías digitales; el artículo dieciséis establece la creación de un banco de pruebas o *Sandbox* multisectorial abierto a todo tipo de innovación; y el artículo diecisiete se centra en la I+D+i de las tecnologías digitales.

El Título Tercero, «Infraestructuras y operadores de comunicaciones electrónicas», consta de cuatro artículos: el artículo dieciocho trata las obligaciones y derechos de los operadores y de la Administración Pública; el artículo diecinueve comprende la sostenibilidad de infraestructuras de operadores de comunicaciones electrónicas; el artículo veinte implanta medidas para las infraestructuras digitales para territorios inteligentes; y el artículo veintiuno corresponde a la fiscalidad en los operadores y prestadores de servicios de telecomunicación.

El Título Cuarto, «Tecnologías para la digitalización», consta de siete capítulos. El Capítulo I, «Robótica Inteligente», comprende cinco artículos: el artículo veintidós incluye la regulación del robot inteligente; el artículo veintitrés establece el marco ético para la robótica inteligente; el artículo veinticuatro determina la coordinación con la Unión Europea en este ámbito; el artículo veinticinco regula los derechos de la propiedad intelectual y flujo de datos; y el artículo veintiséis incluye la responsabilidad y seguridad jurídica aplicada a la tecnología robótica. El Capítulo II, «Sistemas basados en Inteligencia Artificial y *Big Data»,* consta de siete artículos: el artículo veintisiete recoge la responsabilidad de la aplicación de IA; el artículo veintiocho señala el marco ético para los sistemas de IA; el artículo veintinueve establece nuevas funciones del Consejo Asesor de Inteligencia Artificial; el artículo treinta hace referencia a la financiación e incentivos fiscales de aplicación de la IA; el artículo treinta y uno indica las actuaciones sobre los consumidores de sistemas basados en IA; el artículo treinta y dos se refiere al reconocimiento biométrico basado en IA; y el artículo treinta y tres comprende los derechos de propiedad intelectual derivado del uso de IA. El Capítulo III, «Aeronaves no tripuladas. Drones», consta de ocho artículos: el artículo treinta y

cve: BOCG-14-B-173-1

cuatro desarrolla actuaciones necesarias en materia de aeronaves no tripuladas; el artículo treinta y cinco regula el empleo de drones en el sector comercial e industrial, el artículo treinta y seis destaca las actuaciones con respecto al empleo de drones civiles en usos de última milla; el artículo treinta y siete regula el empleo de drones para el servicio postal universal; el artículo treinta y ocho regula el empleo de drones para el transporte de mercancías; el artículo treinta y nueve contempla la normativa municipal; el artículo cuarenta establece los incentivos fiscales en la tecnología de drones; y el artículo cuarenta y uno trata el impacto ambiental del uso de los drones. El Capítulo IV, «Vehículo conectado y parcialmente automatizado», contiene dos artículos: el artículo cuarenta y dos establece las medidas necesarias para la protección de datos; y el artículo cuarenta y tres hace referencia a la protección de los usuarios frente a ciberataques.

El Capítulo V, «Internet de las Cosas (IoT)», comprende dos artículos: el artículo cuarenta y cuatro recoge las obligaciones de los fabricantes de sistemas IoT; y el artículo cuarenta y cinco regula la seguridad en sistemas IoT. El Capítulo VI, «Computación en la nube», comprende dos artículos: el artículo cuarenta y seis, trata de la limitación de responsabilidades; y el artículo cuarenta y siete establece los incentivos para empresas proveedoras de servicios en la nube. El Capítulo VII, *«Blockchain»,* contiene nueve artículos: el artículo cuarenta y ocho establece el ámbito de regulación de las criptomonedas; el artículo cuarenta y nueve recoge las medidas que regulan la Oferta inicial de moneda (ICO); el artículo cincuenta crea el Consejo Nacional de Criptoactivos (CNC) con fines consultivos; el artículo cincuenta y uno incluye medidas en materia de hipotecas, seguros e indemnizaciones; el artículo cincuenta y dos concreta el régimen jurídico general de la tecnología *Blockchain;* el artículo cincuenta y tres hace referencia a las operaciones fraudulentas de blanqueo de capitales y terrorismo; el artículo cincuenta y cuatro menciona la protección del medio ambiente en materia de *Blockchain;* el artículo cincuenta y cinco establece las actuaciones necesarias con respecto a la protección de usuarios; y el artículo cincuenta y seis contempla la fiscalidad.

El Título Quinto, «Protección digital ciudadana», consta de dos capítulos. El Capítulo I, «Derechos digitales y obsolescencia programada», con dos artículos, recoge, en el artículo cincuenta y siete, la protección de los derechos digitales, el derecho a la intimidad y el honor en el ámbito digital; y en el artículo cincuenta y ocho las medidas que regulan la práctica de la obsolescencia programada. El Capítulo II, «Seguridad digital», contiene dos artículos: el artículo cincuenta y nueve establece la protección del menor; y el artículo sesenta crea un cuerpo de Reserva Estratégica de Talento en Ciberseguridad.

TÍTULO PRELIMINAR

Ámbito de aplicación y principios generales

Artículo 1. Objeto de la ley.

La presente ley tiene por objeto establecer las bases del sistema español de transformación digital en España para facilitar el proceso de la empresa hacia la digitalización, desarrollar la competitividad digital, regular el uso de las tecnologías disruptivas o tecnologías clave para la transformación digital de España, regular la fiscalidad asociada a la digitalización del sector empresarial y de las comunicaciones electrónicas, reforzar los derechos digitales de los ciudadanos, de su relación con las administraciones públicas y proteger su seguridad, en el contexto del nuevo modelo de sociedad digital que se ha visto acelerado por la crisis de la COVID-19.

Artículo 2. Ámbito de aplicación.

1. La presente ley será de aplicación:

a) A las entidades que integran el sector público, definido en los términos del artículo 2 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.

b) Al sector privado, comprendiendo tanto las personas jurídicas como las personas físicas que se dediquen a una actividad profesional en el ámbito de la empresa, la tecnología y la digitalización, en particular:

— A las empresas y desarrollad ores de *software* que elaboren soluciones de Inteligencia Artificial y robótica inteligente y a las empresas que lo comercialicen.

cve: BOCG-14-B-173-1

— A los centros dedicados a servicios de computación en la nube.
— A los prestadores de servicios basados en tecnología *Blockchain.*
— A los operadores de Telecomunicación y prestadores de servicios de comunicaciones electrónicas y de servicios digitales.
— A las entidades asociativas de carácter privado con fines públicos o de interés general.
— A los fabricantes de vehículos conectados y de sistemas robóticos.
— A los fabricantes de aeronaves no tripuladas pilotadas por control remoto o autónomas, y a los agentes y operadores del mercado y del sector transporte que realicen usos industriales o usos y operaciones comerciales con ellas. En ningún caso resultará de aplicación a las actividades militares.
— A los empresarios, fabricantes, profesionales y a cualesquiera otras personas físicas o jurídicas que participen en el mercado de productos digitales fabricados para el consumo particular.
— Al resto de entidades de carácter asociativo privado que constituyen la sociedad civil, establecidas en los artículos 1669 y 1678 del Real Decreto, de 24 de julio de 1889, por el que se publica el Código Civil.
— A los consumidores y usuarios para su protección.

Artículo 3. Ámbito territorial.

Las disposiciones de esta ley son aplicables en todo el territorio nacional, sin perjuicio de las competencias que, en su caso, hayan asumido las Comunidades Autónomas en el marco de la Constitución, de los Estatutos de Autonomía y de la legislación del Estado en materia de Hacienda, Agricultura y Ganadería, Ciencia, Consumo, Educación, Economía, Empleo, Innovación, Investigación, Justicia, Medio Ambiente, Seguridad Nacional, Seguridad Vial, Transporte, Tránsito Aéreo, Transformación Digital y Universidades.

Artículo 4. Principios de la Ley.

1. En el ámbito del sector público:

a) Promover un ecosistema favorable para el desarrollo y el uso de las tecnologías esenciales facilitadoras en el ámbito público.
b) Aplicar la tecnología para mejorar los procedimientos administrativos, a través de una Administración Pública Digital enfocada a procurar la agilización de los trámites administrativos.
c) Impulsar la adopción de la Inteligencia Artificial y el uso del Big Data en todos los ámbitos posibles de la economía y de la gestión pública, mejorando las inversiones en investigación e innovación.
d) Favorecer la investigación y el uso de las aeronaves civiles pilotadas por control remoto o autónomas, en el sector industrial y comercial, especialmente en el transporte de mercancías, la prevención de catástrofes y CNMC la conectividad de las zonas rurales.
e) Establecer bases de protección en los ámbitos de la ciberseguridad y la seguridad ciudadana digital.
f) Fomentar el voluntariado tecnológico de apoyo a las necesidades digitales de la sociedad.

2. En el ámbito del sector privado:

a) Incentivar el desarrollo y uso de los sistemas digitales y la aplicación de tecnologías esenciales facilitadoras en el ámbito empresarial.
b) Incentivar el despliegue de infraestructuras digitales de servicios a la ciudadanía y al sector productivo de nuestro país.
c) Integrar, en el sistema empresarial, nuevos modelos de negocio digitales.
d) Certificar la conveniencia y oportunidad de las decisiones tomadas por sistemas basados en Inteligencia Artificial, asegurando la convivencia de las necesidades ciudadanas con esta tecnología.
e) Establecer medidas que eviten la obsolescencia programada de productos digitales, evitando los daños medioambientales de esta práctica como el agotamiento de los recursos y la generación de residuos contaminantes.
f) Internacionalizar la Industria digital española dentro del entorno europeo.
g) Diseñar un marco legal para el uso de la tecnología *Blockchain y* los criptoactivos, estableciendo sus parámetros de utilización y favoreciendo su implantación en entidades públicas y privadas, evitando fraudes y malas prácticas en el uso de esta tecnología y en el de las criptomonedas.

cve: BOCG-14-B-173-1

3. En el ámbito de los ciudadanos:

a) Incentivar el conocimiento y uso de los sistemas digitales y la aplicación de tecnologías disruptivas.
b) Promover la formación de los ciudadanos en el mundo digital y el acceso a la tecnología.
c) Asegurar la convivencia con sistemas basados en inteligencia artificial, eliminado los riesgos asociados a las malas prácticas y sesgos potenciales en la implementación de esta tecnología.
d) Garantizar la seguridad informática de los usuarios en la red, especialmente de los menores de edad en el uso de internet.
e) Asegurar que las operaciones realizadas con criptomonedas se realicen en un marco de confianza, seguridad y transparencia.
f) Adaptar los planes educativos y la formación de los trabajadores a los cambios del mercado laboral y al teletrabajo, favoreciendo el talento tecnológico y fomentando el uso educativo y social de los videojuegos.

Artículo 5. Definiciones.

A los efectos de lo dispuesto en esta Ley, se entenderá por:

— «Aerovía»: Volumen del espacio aéreo que a modo de corredor de transporte se establece para la navegación aérea y, particularmente, la navegación de d rones.
— «Algoritmo»: Conjunto ordenado de operaciones sistemáticas que permite realizar un cálculo y hallar la solución de un problema.
— «Automatización»: Sistema donde se transfieren tareas de producción, realizadas habitualmente por operadores, a un conjunto de elementos tecnológicos.
— *«Big Data»:* Cantidad voluminosa de datos estructurados, semiestructurados y no estructurados que tienen el potencial de ser extraídos y procesados para obtener información.
— *«Blockchain»:* Tipo de libro de registros distribuido, de todas las operaciones que se realizan en la red en un tiempo determinado. Funciona como una base de datos descentralizada y administrada por computadores pertenecientes a una red de punto a punto o P2P *(peer-to-peer).* Los mecanismos de consenso y la criptografía garantizan la seguridad de la red, no pudiendo eliminar ni modificar nada sin el consenso de la mayoría de los participantes de la red.
— «Brecha digital»: Diferencia que existe entre las personas que utilizan las Tecnologías de la Información y las Comunicaciones (TIC) como una parte rutinaria de su vida diaria frente a aquéllas que no tienen acceso a las mismas, por motivos geográficos o socioeconómicos, o que no tienen habilidad o conocimiento para su uso.
— «Casas de cambio»: Entidades que permiten a los clientes cambiar una divisa por otra, incluyendo criptodivisas.
— «Ciberdefensa»: Conjunto de tecnologías que se utilizan para prevenir las amenazas, como el ciberterrorismo o el cibercrimen, y dar respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad nacional.
— «Ciberespacio»: Dominio digital que ha de ser defendido, según la Estrategia de Seguridad Nacional, con la misma intensidad que el resto de los dominios tales como la tierra, el mar, el aire y el espacio.
— «Ciberseguridad»: Conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información en Internet y la protección de los ordenadores, servidores, dispositivos electrónicos, redes y datos informáticos de ataques maliciosos. Dicho término abarca numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final.
— *«Cloud»:* Tecnología que permite a un usuario almacenar todos los archivos e información en Internet (nube).
— *«Cloud Computing»:* Tecnología de computación en la nube que permite acceso remoto a *software,* almacenamiento de archivos y procesamiento de datos por medio de Internet.
— «Criptoactivo»: Conjunto de criptodivisas y otras formas de bienes y servicios (criptomonedas, *tokens,* contratos inteligentes o sistemas de gobernanza) que utilizan la tecnología *Blockchain* y la criptografía (tipo de escritura que funciona con cifras o códigos secretos).

cve: BOCG-14-B-173-1

— «Criptomoneda»: Moneda virtual, que puede ser intercambiada y operada como cualquier otra divisa tradicional, salvo que está fuera del control de las entidades bancarias y Estados. Las criptomonedas son un subconjunto de las monedas digitales basadas en la criptografía.

— «Crowdfunding»: Llamado micromecenazgo, en castellano, es un mecanismo colaborativo de financiación de proyectos desarrollado sobre la base de las nuevas tecnologías.

— «Crowdlending»: Préstamos ofertados de particulares a otros particulares sin la intervención de una institución financiera tradicional. En muchos casos se trata de microcrédito.

— «Dron»: Aeronave no tripulada capaz de mantener, de manera autónoma o por control remoto, un nivel de vuelo controlado y sostenido.

— «Economía basada en datos»: Empresa que utiliza un enfoque *«data-driven»* (impulsado por datos, en castellano), para la toma de decisiones estratégicas basadas en análisis de datos e interpretación, permitiendo atender mejor a sus clientes y consumidores.

— «Entidades de capital riesgo»: Entidades financieras para la adquisición de participaciones temporales en el capital de empresas no financieras y que no coticen en bolsa en el momento de dichas adquisiciones.

— «Espacio aéreo segregado»: Volumen definido de espacio aéreo para uso específico de una actividad.

— *«Exchange»:* Servicios de cambio de moneda virtual en moneda fiduciaria.

— «Fondo de Capital Riesgo»: Institución de inversión colectiva, enfocada a invertir capital en empresas, preferentemente, *startups,* con gran capacidad potencial de crecimiento acelerado de la innovación.

— *«Initial Coin Offering,* ICO»: Medio de financiación de proyectos empresariales a través de criptomonedas.

— «Infraestructura de comunicaciones dedicada»: Infraestructura de red de comunicaciones electrónicas de uso específico para una función o sector concreto.

— «Inteligencia Artificial, IA»: Inteligencia exhibida por máquinas gracias a la combinación de algoritmos de aprendizaje autónomo a partir de datos.

— «Internet de las cosas (IoT)»: Interconexión digital dçe objetos cotidianos, dotados de conectividad, a través de Internet u otras redes dedicadas.

— *«Machine Learning»:* Disciplina científica del ámbito de la Inteligencia Artificial, que crea sistemas que aprenden autónomamente.

— *«Massive Open Online Course* (MOOC)»: Cursos en línea, masivos y abiertos bajo una una modalidad de formación y aprendizaje dirigido a un número masivo de usuarios en temas específicos, de acceso libre, abierto y gratuito para promover el aprendizaje autónomo.

— «Operador de Telecomunicaciones»: Cualquier empresa legalmente constituida que cuenta con las licencias, permisos y garantías exigidas por Ley para ejercer actividades de telecomunicaciones con consumidores finales personas físicas u otras personas jurídicas (administraciones, empresas, organismos, etc.).

— «OTT»: Servicio de libre transmisión *(Over the Top),* que hace referencia a plataformas que emiten contenido a través de Internet sin necesidad de recurrir a operadores tradicionales de difusión.

— «Prestador de Servicios de Comunicaciones Electrónicas»: Toda persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público.

— *«Private Equity»:* Fondos de inversión dedicados, fundamentalmente, a *StartUps* innovadoras, a cambio de controlar un porcentaje de la empresa o de sus acciones.

— «PYME»: Empresa pequeña o mediana en cuanto a volumen de ingresos, valor del patrimonio y número de trabajadores.

— «Responsabilidad jurídica»: Responsabilidad atribuida a un sujeto por un daño que ha sufrido una persona (física o jurídica) o un bien jurídico.

— «Robot»: Máquina automática programable capaz de realizar determinadas operaciones de manera autónoma, pudiendo reemplazar tareas habitualmente ejercidas por personas, especialmente las pesadas, repetitivas o peligrosas.

— *«SandBox»:* Espacio de prueba cerrado y controlado en el que los operadores o desarrolladores pueden experimentar y validar un producto o servicio, en un entorno ya regulado, ejecutando programas de forma segura y sin riesgo para ese entorno o usuarios.

cve: BOCG-14-B-173-1

— «Seguridad de la información»: Conjunto de medidas preventivas y reactivas de las organizaciones y los sistemas tecnológicos que permiten proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

— *«Serious Games»:* También denominados «juegos serios», son videojuegos con un propósito capacitativo o educativo. El término «serio» hace referencia a todos aquellos videojuegos que se utilizan en el sector industrial, educativo, científico, sanitario o formación profesional.

— «Sistema ADAS»: El Sistema Avanzado de Apoyo a la Conducción es un conjunto de tecnologías basadas en sensores, IA y conectividad que ayudan a reducir los riesgos que aparecen cuando se circula, tanto para el propio conductor y demás ocupantes del coche, como para el resto de usuarios de la vía.

— *«Smart Contract»:* Acuerdo entre partes, con capacidad para autoejecutarse mediante un código informático. *Blockchain* confirma que se dan las condiciones sobre el cumplimiento o no del contrato en los términos acordados y lo resuelve de forma independiente o con ayuda de elementos externos, como las fuentes de datos externas denominadas oráculos. Permite obtener certeza indubitada sobre fechas, horas, datos, etc. y mejorar el coste asociado a la seguridad jurídica en las transacciones.

— *«Software»:* Conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora o dispositivo electrónico.

— *«Startups»:* Término utilizado para designar a empresas emergentes con ideas innovadoras que se apoyan en las nuevas tecnologías.

— «Tecnologías Disruptivas»: Aquellas nuevas tecnologías o innovaciones *(Big Data,* Inteligencia Artificial, nanotecnología, drones, Internet de las Cosas, impresión 3D, etc.) que permiten fabricar o desarrollar servicios que no pueden alcanzarse con tecnologías tradicionales.

— «Tecnologías esenciales facilitadoras»: Aquéllas que proporcionan elementos tecnológicos indispensables que permiten el desarrollo de una amplia gama de nuevos materiales, productos, procesos y servicios de mayor valor añadido. Se incluyen la microelectrónica, nanoelectrónica, fotónica, nanotecnología, biotecnología, materiales y los sistemas de fabricación avanzados.

— *«Token»:* Ficha que puede ser canjeada por una criptomoneda, servicio, producto, derecho en la empresa, participación en acciones, etc.

— «Trazabilidad»: Sistema que se basa en el registro de huellas que deja un producto durante su tránsito por la cadena antes de llegar al consumidor.

— «Usos de última milla»: Empleo de los drones como parte de una ruta logística de distribución de mercancías a fin de lograr el suministro de los bienes hasta sus receptores finales en el punto acordado de recogida.

— «Usos industriales (drones)»: Uso de los drones que implican la realización de rutas dentro de un volumen del espacio aéreo perfectamente delimitado, sin rebasarlo bajo ningún concepto y asociado a otra actividad industrial principal diferente de la propia navegación aérea.

— «Vehículo aéreo no tripulado»: *Unmanned Aerial System* (UAS, en sus siglas en inglés,) se refiere a una aeronave que vuela sin tripulación y que ejerce su función por remoto.

— «Vehículo conectado»: Aquel vehículo que se equipa de aplicaciones, servicios y tecnologías que lo conectan con su entorno.

— «Vehículo parcialmente automatizado»: También conocido como vehículo de Nivel 2 de automatización, es un vehículo que puede controlar el movimiento lateral y longitudinal sin necesidad de un piloto automático, lo que exige un nivel constante de atención por parte del conductor.

— *«Venture Capital»:* Inversiones que, a través de acciones, sirven para financiar, fundamentalmente, *startups* innovadoras desde su primera fase de su desarrollo.

TÍTULO PRIMERO

Gobernanza de la Transformación Digital en España

Artículo 6. Administración Pública Digital.

1. Las Administraciones Públicas incorporarán herramientas digitales, tales como *Big Data* e Inteligencia Artificial, para mejorar las políticas públicas en ámbitos como la salud pública, transporte, educación, empleo, medio ambiente, condiciones de salubridad, alimentación y cualquier otra que afecte a la ciudadanía.

cve: BOCG-14-B-173-1

2. Los sistemas de información y gestión de datos utilizados por las Administraciones Públicas garantizarán la compatibilidad e interoperabilidad con otros sistemas y aplicaciones utilizados, sea cual fuere la tecnología de acceso, dispositivo o aplicación.

3. Las Administraciones Públicas promoverán e invertirán en el uso de las soluciones *Cloud* para mejorar la eficiencia de sus actuaciones y reducir el impacto ambiental.

4. En cuanto a la Protección de Datos, las Administraciones Públicas, en el ámbito de sus competencias, emprenderán las siguientes acciones:

a) Promover las iniciativas europeas destinadas a crear un entorno competitivo justo en el uso de los datos.

b) Velar por el equilibrio entre privacidad e innovación en el mundo digital basado en el dato.

c) Evitar el establecimiento de marcos de restricción distintos para las diferentes empresas del ecosistema digital.

d) Optimizar la reducción de la burocracia innecesaria y promover la reducción de cargas administrativas, poniendo a disposición de los ciudadanos y las empresas las infraestructuras digitales necesarias para una eficaz gestión.

Artículo 7. Oficina Técnica para la Financiación Digital.

Se crea la Oficina Técnica para la Financiación Digital, dependiente del Ministerio de Hacienda, formada por representantes de organismos públicos y privados, que tendrá entre sus funciones:

1. Optimizar la gestión de los fondos públicos destinados al sector tecnológico y digital provenientes de la Unión Europea.

2. Asesorar la gestión de los fondos europeos destinados a la digitalización.

3. Participar en la valoración de las diferentes propuestas de digitalización que se presenten desde España para la concesión de fondos europeos.

Artículo 8. Gobernanza para la digitalización.

Las Administraciones Públicas, en el ámbito de sus competencias, llevarán a cabo las siguientes acciones:

1. Promover un desarrollo normativo para la cooperación, coordinación y equiparación de las políticas destinadas a la digitalización y a la disminución de las brechas digitales entre las Comunidades Autónomas y el Gobierno de España.

2. Fomentar la compra de tecnologías innovadoras destinadas a la digitalización.

3. Habilitar la utilización por parte de las empresas de las infraestructuras públicas existentes de I+D+i, centros empresariales, centros de demostración avanzada e Infraestructuras Científicas y Técnicas Singulares (ICTS).

4. Crear un certificado de sello de calidad de la industria española digital, incorporando sus requisitos e instrumentos de control.

5. Promover la estandarización internacional de procesos, la formación de los trabajadores en el ámbito digital y una digitalización coherente con la economía circular.

6. Apoyar financieramente a las empresas que inviertan en tecnología para adaptar sus equipos al teletrabajo y en formación en ciberseguridad, en proteger el acceso a los datos de la empresa y a sus documentos y en salvaguardar los derechos de sus clientes respecto a la seguridad de las transacciones.

7. Priorizar los trámites para la apertura y creación de empresas y negocios a través de herramientas digitales seguras y que nunca superarán el plazo de 48 horas desde su solicitud, siempre y cuando se cumplan los requisitos legales establecidos en cada caso.

8. Desarrollar modelos que potencien el uso eficaz de la información para crear una economía basada en datos entorno a sectores clave para el PIB español y referentes a nivel internacional.

9. Establecer incentivos fiscales a las empresas que investiguen en tecnologías para reducir el impacto medioambiental y el consumo de recursos de servicios de IoT, *Cloud Computing* o *Big Data.*

10. Desarrollar, hasta la plena implementación y la total interoperabilidad en toda España, el modelo de historia clínica digital del Sistema Nacional de Salud, que incluya la documentación clínica necesaria

cve: BOCG-14-B-173-1

para garantizar una atención sanitaria de calidad, con independencia del lugar del territorio nacional en el que se encuentre el paciente, así como facilitar la labor de los profesionales sanitarios.

11. Fomentar los cauces necesarios para garantizar el pleno acceso y la total disponibilidad de los pacientes a la información relativa a su historia clínica, mediante el uso de estas tecnologías, favoreciendo además la creación de canales digitales eficaces para la comunicación directa y la consulta con los profesionales sanitarios.

12. Elaborar un mapa actualizado de inventario de las capacidades industriales y tecnológicas de las Comunidades Autónomas, relacionado con las necesidades sanitarias, creando una reserva estratégica de equipamiento que permita dar una solución diligente ante situaciones de emergencia como pandemias u otras catástrofes, sin depender de terceros países.

Artículo 9. Consejo Consultivo para la Transformación Digital.

El Consejo Consultivo para la Transformación Digital, además de las funciones que legalmente tiene encomendadas, desarrollará los siguientes cometidos:

1. Fomentar los planes de formación digital para aquellos trabajadores cuyos puestos pueden ser reemplazados por tecnologías emergentes por causas de transformación digital de sus empresas.

2. Incentivar la formación de directivos y trabajadores industriales en la tecnología de *Big Data,* robótica avanzada e inteligencia artificial.

3. Realizar el seguimiento de los indicadores que recojan el nivel de implementación de las medidas para la digitalización.

TÍTULO SEGUNDO

Competitividad y competencias digitales

Artículo 10. Plan para la digitalización de las PYMES.

1. Se crea el «certificado cien por cien digital», que supone la certificación oficial de calidad digital de las PYMEs españolas y la garantía del cumplimiento de los requisitos de producción e innovación en el marco de unos parámetros de sostenibilidad.

2. El «certificado cien por cien digital» está asociado a incentivos fiscales.

3. En el plazo de dos años desde la publicación de la presente ley, las convocatorias de subvenciones y ayudas públicas dirigidas a las PYMEs incluirán en sus requisitos la posesión del «certificado cien por cien digital».

4. Para obtener el «certificado cien por cien digital» las empresas presentarán la ejecución de un Plan de Digitalización, que comprenderá:

a) Inversiones realizadas para incrementar las soluciones digitales de la gestión empresarial, poniendo énfasis en la innovación tecnológica, la organización avanzada de los recursos humanos, el desarrollo del capital humano, la participación y la transparencia.

b) Actualización de los equipos informáticos, dispositivos y conexión a la red.

c) Descripción de un programa informático de facturación electrónica, conforme a los requisitos de las administraciones públicas.

d) Utilización de la tecnología digital para modernizar las áreas funcionales que conforman la empresa y automatizar los procesos, estrategias, modelos de negocio, operaciones, productos, marketing, objetivos, etc.

e) Existencia de un plan de retención y atracción del talento digital.

f) Implantación de un sistema de seguridad informática, tanto en la red como en los equipos y dispositivos físicos locales, que impida el ciberataque o cualquier otra acción maliciosa.

g) Elaboración de planes de formación en tecnologías emergentes para los trabajadores en activo.

h) Adaptación de la tecnología de equipos y aplicaciones al teletrabajo y establecer políticas de conciliación familiar y laboral.

cve: BOCG-14-B-173-1

Artículo 11. Financiación.

1. Respecto a la financiación, las Administraciones Públicas, en el ámbito de sus competencias, supervisarán y controlarán el cumplimiento de las medidas establecidas en el Plan España Digital 2025 y realizarán las siguientes acciones:

a) Apoyar a aquellas PYMES que, siendo capaces de ejecutar un contrato por su capacidad técnica, no tienen un balance que respalde la emisión de los avales que se emiten en la firma de los contratos internacionales.
b) Creación de un «Fondo Capital Semilla», destinado a las subvenciones y ayudas financieras o no financieras, avales, etc. de las empresas tecnológicas, conforme a los principios de concurrencia, objetividad y no discriminación.
c) Creación de un plan de incentivos fiscales para las empresas con el sello «cien por cien digital».

2. Las Administraciones Públicas, en el ámbito de sus competencias, realizarán las siguientes acciones:

a) Facilitar el acceso a la financiación bancaria y no bancaria para apoyar la transformación digital de las empresas.
b) Impulsar los mercados alternativos de valores, bursátil y de renta fija, así como fomentar capital riesgo, el sistema de garantías y otras vías de financiación no convencional.
c) Mejorar las condiciones que permitan la autofinanciación de las empresas y reducir la morosidad de sus cobros.

Artículo 12. Fiscalidad.

Respecto a la fiscalidad, las Administraciones Públicas, en el ámbito de sus competencias, realizarán las siguientes acciones:

1. Adaptar la normativa española a la que se establezca para la Unión Europea, impidiendo que se incorporen en España cargas fiscales que no hayan sido objeto de procesos de armonización fiscal supranacional.
2. Elaborar un marco normativo que reduzca la complejidad impositiva y disminuya la inseguridad jurídica.
3. Revisar y reorganizar el actual marco tributario y analizar las principales cargas tributarias que afectan de manera específica al sector de la economía digital en España y a las compañías tecnológicas.

Artículo 13. Responsabilidad social de las empresas.

El Ministerio que tenga entre sus competencias la Transformación Digital convocará premios a la excelencia digital y buenas prácticas en materia tecnológica, en el marco de los Objetivos de Desarrollo Sostenible del Programa de las Naciones Unidas para el Desarrollo, en convocatorias específicas para ello.

Artículo 14. Competencias digitales.

1. Las Administraciones Públicas, en el ámbito de sus competencias, establecerán las acciones necesarias para adaptar la realidad formativa y laboral a los nuevos perfiles tecnológicos.
2. En el ámbito educativo, se realizarán las siguientes acciones:

a) Desarrollar en el alumnado de las diferentes etapas educativas, desde infantil hasta formación profesional y bachillerato, las competencias clave y habilidades en el uso de las tecnologías digitales, programación y robótica básica.
b) Establecer la formación inicial y permanente necesaria para que todos los docentes adquieran el reconocimiento en competencias digitales, conforme al Marco Común de Referencia de la Competencia Digital Docente.

cve: BOCG-14-B-173-1

c) Desarrollar una Estrategia Nacional de Innovación Educativa Digital que permita la creación de un marco de reconocimiento e incentivos de los centros y del profesorado que aporten innovación digital docente, dotándolos de recursos y herramientas tecnológicas.

d) Establecer un programa de implementación completa del proyecto nacional «Escuelas Conectadas», que permita dotar a centros educativos de una conectividad de calidad y de la interoperabilidad de los sistemas, cuyo desarrollo y puesta en marcha suponga la base sobre la que construir la digitalización de la formación.

e) Intensificar las enseñanzas en Ciencia, Tecnología, Ingeniería y Matemáticas (STEM), en todas las etapas educativas, así como fomentar las vocaciones y el talento científico.

f) En la Formación Profesional, adaptar las titulaciones educativas a las necesidades de la sociedad digital, actualizar los mapas de empleabilidad de las mismas, potenciar las especialidades STEM entre los jóvenes, promoviendo el equipamiento y el uso de las tecnologías digitales desde las primeras etapas educativas.

g) Apoyar las prácticas pedagógicas innovadoras, en lo que se refiere al modo de integrar y utilizar las herramientas digitales, la IA en las aulas y los *Serious Games.*

h) Fomentar el uso responsable y adecuado de los recursos digitales, garantizando la protección de la infancia y la adolescencia frente al ciberacoso y otros delitos informáticos.

i) En el ámbito universitario, sin perjuicio de la propia autonomía universitaria española, destinar los recursos necesarios tanto para la formación de los docentes en la adquisición de los conocimientos, competencias y herramientas en el uso de los recursos didácticos y en la metodología *on line,* como para la digitalización de recursos bibliográficos, la actualización científica y didáctica y la plena interoperabilidad didáctica de los sistemas.

j) Financiar y promover el diseño de grados universitarios que utilicen metodologías para la formación *online* y la oferta en todas las titulaciones de asignaturas optativas en competencias digitales.

3. En el ámbito laboral se realizarán las siguientes acciones:

a) Impulsar la creación de contenidos digitales dirigidos a mejorar las competencias digitales de las empresas. Para ello, se promoverá y financiará, en el ámbito educativo y de empresas dedicadas a la formación, el desarrollo de cursos *MOOCs,* para la educación en los nuevos conocimientos digitales, estableciendo sinergias entre la educación formal y las empresas e instituciones que demandan dichos conocimientos.

b) Establecer incentivos fiscales que fomenten la inversión de las empresas en la formación digital de sus empleados, adaptando la normativa existente a la nueva realidad pedagógica del mercado de trabajo y la estrategia de las empresas.

c) Aumentar las oportunidades formativas de los trabajadores y del conjunto de ciudadanos a través de préstamos subsidiados, o con intereses muy bajos, para la educación, programas de becas y medidas fiscales.

d) Incluir las Comisiones Paritarias Sectoriales (CPS), como garantes del consenso entre asociaciones empresarias y sindicales para la elaboración de los planes de formación y del modelo de cualificaciones profesionales, así como de la demanda real del mercado laboral en materia digital.

e) Diseñar un sistema de recogida de necesidades formativas que dé respuesta a los sectores dinámicos y cambiantes y que permita anticiparse a las nuevas necesidades.

4. En el ámbito profesional, se establecerá un sello de acreditación profesional, homogéneo en todo el territorio español, que certifique las competencias y capacidades profesionales en el ámbito de las tecnologías disruptivas digitales, que serán evaluadas por los Colegios Profesionales o los Consejos Generales de las titulaciones correspondientes, incentivando el reconocimiento laboral, la experiencia y la mejora continua de los profesionales en el ámbito de la digitalización.

Artículo 15. Startups de base tecnológica.

1. Las Administraciones Públicas, en el ámbito de sus competencias, simplificarán, mediante la digitalización, los trámites relacionados con la constitución, puesta en marcha, traspaso o cierre de una *startup,* en el plazo de 48 horas.

cve: BOCG-14-B-173-1

2. Las Administraciones Públicas, en el ámbito de sus competencias, promoverán medidas para la financiación directa a emprendedores y financiación a agentes privados para su inversión en emprendimiento, impulsará el micromecenazgo *(crowdfunding,* en inglés) y la financiación colectiva *(crowdlending,* en inglés) e incorporará medidas de transparencia que ayuden a limitar los riesgos para los inversores y aumentar los límites de inversión.

3. Respecto a la contratación de talento extranjero, las Administraciones Públicas, en el ámbito de sus competencias, simplificarán y facilitarán los medios necesarios para la acreditación de medios económicos, materiales y personales para el proyecto empresarial, con el fin de facilitar su incorporación en el ámbito de la empresa, la universidad o la investigación.

4. Durante los dos primeros ejercicios fiscales, desde la constitución de una *startup,* la cuota del Impuesto de Sociedades tendrá una bonificación del 50 %.

5. Las acciones o participaciones de las *startups* que, de forma gratuita o por debajo de su precio de mercado, se entreguen a sus trabajadores estarán exentas de su declaración como rendimiento del trabajo.

6. Se podrán ofertar acciones o participaciones a los trabajadores de una *StartUp,* en condiciones diferentes, a criterio de la compañía.

7. El trabajador mantendrá las acciones y su condición de trabajador durante dos años salvo fallecimiento, incapacidad permanente, cierre de la empresa, operación corporativa o salida a cotización bursátil en ese periodo.

8. Se creará una exención en el IRPF del 100 % de la plusvalía obtenida siempre que el importe íntegro de la enajenación se reinvierta en la suscripción de acciones o participaciones de otra *startup* y una exención parcial en caso de reinversión parcial, en un plazo de 4 años.

9. Se modificará en la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva, de manera que se optimice el tratamiento normativo y fiscal del retorno adicional de la Inversión de los gestores en los fondos que gestionan, adecuándolo al de los principales países de nuestro entorno.

10. Se facilitará el acceso de inversores no profesionales en entidades de *Venture Capital,* fomentando el acceso a este tipo de productos a inversores minoristas no profesionales, evitando la actual rigidez de los criterios objetivos para calificar al «inversor profesional», modificando el artículo 72 de la Ley 22/2014, que regula las entidades de capital-riesgo.

11. Las Administraciones Públicas, en el ámbito de sus competencias, establecerán incentivos fiscales a la inversión por parte de personas jurídicas y físicas. Para ello, se extenderá a las personas físicas, la deducción del 20 % en el IRPF sobre el capital invertido, en el caso de participar en Entidades de Capital Riesgo especializadas en *Venture Capital.*

Artículo 16. *Sandbox* multisectorial.

1. Se promoverá la creación de un *Sandbox* multisectorial, abierto a todo tipo de innovación, que permita crear condiciones seguras para que puedan probarse innovaciones de base tecnológica bajo vigilancia de los supervisores.

2. Una compañía ya existente, que se ajuste a los requisitos legales vigentes, podrá utilizar este nuevo marco *Sandbox* para poner en marcha un proyecto de innovación, confirmar su viabilidad y su funcionamiento o desecharla en caso de que no funcione según lo esperado.

3. Podrá utilizar un *Sandbox* toda aquella compañía o empresa que tenga una idea original que pueda ser probada en un entorno regulado, con el fin de impulsar a las empresas que apuesten por la transformación digital en los sectores actualmente regulados en España, además del financiero.

Artículo 17. I+D+i en tecnologías digitales.

1. Las Administraciones Públicas, en el ámbito de sus competencias, realizarán las siguientes acciones:

a) Desarrollar y hacer público un calendario de inversiones para alcanzar y consolidar, en ejercicios posteriores, el objetivo de destinar un mínimo del 2 por ciento del PIB en I+D+i potenciando el porcentaje de gasto en innovación del sector privado.

b) Facilitar a las empresas digitales el acceso a Instalaciones Científico Tecnológicas Singulares (ICTS), especialmente en sus etapas más tempranas y con mayor riesgo de mercado.

cve: BOCG-14-B-173-1

c) Promover una gestión eficiente de la propiedad intelectual e industrial que proteja la investigación, el desarrollo y el despegue de las empresas digitales.

2. Los proyectos de *software* que incorporen Inteligencia Artificial participarán de las deducciones para incentivar la realización de determinadas actividades, establecidas en el artículo 35 del Real Decreto Legislativo 4/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Impuesto sobre Sociedades.

3. Los gastos inherentes al registro de la propiedad industrial y a la Certificación Entidad Nacional de Acreditación (ENAC) de los proyectos de I+D+I serán considerados como actuaciones de «Innovación Tecnológica» a efectos de Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades.

4. Las *startups* en el proceso de explotación de la innovación tecnológica tendrán una reducción del 90 % del coste de las tasas del Registro de Patentes y modelo de utilidad de ámbito nacional en la Oficina de Patentes y Marcas.

TÍTULO TERCERO

Infraestructuras y operadores de comunicaciones electrónicas

Artículo 18. Derechos y obligaciones.

1. Las autoridades regulatorias tendrán la obligación de confeccionar una memoria de empleo donde se mida el impacto real que cualquier novedad en las obligaciones para con los operadores de comunicaciones electrónicas.

2. Las Administraciones Públicas, en el ámbito de sus competencias, impulsarán, en la Unión Europea, la cooperación horizontal y la compra conjunta de derechos de explotación multiterritorial, de manera que los operadores locales europeos puedan competir con los grupos digitales globales.

3. La Administración Pública, en el ámbito de sus competencias, establecerán medidas de fomento de empleo en todos los procesos de licitación para la explotación del espectro radioeléctrico e infraestructuras, priorizando sobre cualquier modelo de recaudación económica.

Artículo 19. Sostenibilidad de infraestructuras de operadores de comunicaciones electrónicas.

Las Administraciones Públicas, en el ámbito de sus competencias, establecerán medidas adicionales que tengan en cuenta la necesaria sostenibilidad de las inversiones y disminuyan el impacto de infraestructuras en territorios poco poblados de gran riqueza natural o cultural.

Artículo 20. Infraestructuras digitales para territorios inteligentes.

Las Administraciones Públicas, en el ámbito de sus competencias, promoverán iniciativas para facilitar y agilizar el despliegue de Infraestructuras digitales dentro de su territorio, acorde a las siguientes actuaciones:

1. Desarrollar medidas de simplificación y agilidad administrativa, revisando la legislación vigente o promoviendo nuevas normativas para garantizar el despliegue de infraestructuras digitales en núcleos urbanos.

2. Elaborar un plan de desarrollo de las zonas rurales que permita y garantice la configuración del «Pueblo Inteligente» o *Smart Village,* y que incluya conectividad de banda ancha, medidas de apoyo fiscales, reducción de cuotas de autónomos, ayudas para la creación de empresas y centros de trabajo colaborativo o *coworking.* El plan de desarrollo contendrá incentivos fiscales que estimulen la captación de empresas digitales innovadoras en el ámbito rural.

3. Identificar las zonas rurales españolas potenciales para implantar este tipo de proyectos, utilizando las soluciones que ofrecen las tecnologías digitales.

Artículo 21. Fiscalidad en los operadores y prestadores de servicios de telecomunicación.

1. Se sustituyen los epígrafes de la sección 76 de las Tarifas del IAE (Impuesto de Actividades Económicas) por un sólo epígrafe 761 denominado «Comunicaciones electrónicas».

cve: BOCG-14-B-173-1

2. La carga fiscal de los ingresos de explotación de los prestadores de servicios de comunicaciones electrónicas como contribución a la Tasa General de operadores será de 0,5 por mil.

3. Se establece en 0,02 euros la tasa por numeración, direccionamiento y denominación que establece la Ley 9/2014, de 9 de mayo, General Telecomunicaciones.

TÍTULO CUARTO

Tecnologías para la digitalización

CAPÍTULO I

Robótica inteligente

Artículo 22. Robot inteligente.

1. Tendrá la consideración de robot inteligente, aquellos dispositivos robóticos que tengan la capacidad de adquirir autonomía mediante sensores o mediante el intercambio de datos con su entorno y de procesar y analizar dichos datos, permitiendo el autoaprendizaje a partir de la experiencia y la interacción.

2. Los usuarios de robots inteligente dispondrán de licencias de uso que se asignarán a cada robot específico, sea de uso personal o industrial, y que será expedido por la Administración Pública a la que corresponda esta competencia, previa valoración de los requisitos que se establezcan.

Artículo 23. Marco ético para la robótica inteligente.

1. El Ministerio, con competencias en Inteligencia Artificial, a propuesta de un grupo de expertos formados, entre otros, por representantes del sector privado, aprobará un código ético de la robótica, basado en la seguridad y salud, la libertad, la intimidad, la integridad, la dignidad, la justicia, la equidad, la autodeterminación, la no discriminación, la no estigmatización, la protección de datos personales, la transparencia y la responsabilidad de los ciudadanos.

2. La responsabilidad de las actuaciones llevadas a cabo por los robots recaerá siempre en los fabricantes que diseñen o comercialicen los productos o servicios que utilicen esta tecnología. Los robots se fabricarán de forma que sea posible conocer, inequívocamente, al legalmente responsable de su comportamiento.

3. Los fabricantes de robots inteligentes están obligados a garantizar el derecho de los trabajadores a su seguridad, además de su protección. Los criterios de seguridad y precaución son de aplicación en las empresas de robótica, tanto en la fase experimental de laboratorio como en los ensayos de robots en situaciones reales.

4. La transferencia de la investigación en IA y la robótica a la puesta en el mercado, se realizará tras las oportunas evaluaciones de seguridad establecidas por las Administraciones Públicas competentes para ello.

Artículo 24. Coordinación con la Unión Europea.

Las Administraciones Públicas, en el ámbito de sus competencias, realizarán las siguientes acciones:

1. Establecer un marco ético y jurídico común para la tecnología de robótica inteligente, basado en los valores de la Unión Europea y en consonancia con la Carta de los Derechos Fundamentales.

2. Colaborar en la creación de una Agencia Europea para la regulación de los principios éticos de la robótica, determinar las normas en materia de mejores prácticas, definir nuevos principios y hacer frente a posibles problemas de protección de los consumidores y desafíos sistémicos.

Artículo 25. Derechos de propiedad intelectual y flujo de datos.

1. Las disposiciones jurídicas relativas al campo específico de la robótica se elaborarán conforme a la normativa vigente de propiedad intelectual.

cve: BOCG-14-B-173-1

2. En el sector de la robótica inteligente, será de aplicación la legislación civil relativa al principio general de protección de datos.

Artículo 26. Responsabilidad y seguridad jurídica.

1. Las Administraciones Públicas, en el ámbito de sus competencias, evaluarán el impacto legislativo del uso de los robots inteligentes y considerarán la posibilidad de establecer un régimen de seguro obligatorio en los casos en que sea pertinente y necesario para categorías específicas de robots, obligando a los fabricantes o a los propietarios de robots a suscribir un contrato de seguro por los posibles daños y perjuicios causados por sus robots inteligentes.
2. Los datos personales procesados por robots estarán obligados al cumplimiento del Reglamento General de Protección de Datos de la UE (2016/679).

CAPÍTULO II

Sistemas basados en Inteligencia Artificial y *Big Data*

Artículo 27. Responsabilidad de la aplicación de IA en los sistemas.

1. La aplicación de la IA, en la sociedad española, se realizará con pleno respeto a los derechos y libertades previstas en la constitución española, protegiendo a los ciudadanos de los posibles efectos y delimitando responsabilidades.
2. Los sistemas de IA, aunque sean capaces de sostener conversaciones complejas con personas a través de programas computacionales serán convenientemente identificados para evitar la suplantación de identidad humana.

Artículo 28. Marco ético para los sistemas de IA.

1. El Ministerio, que tenga entre sus competencias la IA, elaborará un marco ético por el que se rija el funcionamiento de los robots inteligentes o de cualquier otro sistema que posea inteligencia artificial, para lo que contará con expertos en investigación y desarrollo en IA del ámbito privado.
2. Los sistemas de IA se diseñarán de manera que respeten el Estado de Derecho, los derechos humanos, los valores democráticos y la diversidad, e incorporen las salvaguardias adecuadas para garantizar una sociedad justa y equitativa.
3. Las organizaciones y las personas que desarrollen, desplieguen o gestionen sistemas de IA responderán de su correcto funcionamiento en consonancia con el presente marco ético.
4. Los fabricantes de cualquier sistema basado en IA, desarrollarán un protocolo de desactivación para que los usuarios puedan recuperar su control en caso de peligro potencial.

Artículo 29. Consejo Asesor de Inteligencia Artificial.

1. El Consejo Asesor de Inteligencia Artificial queda establecido en la Orden ETD/920/2020, de 28 de septiembre.
2. Dicho Consejo incluirá entre sus funciones, además de las ya previstas en la citada Orden, la supervisión del sistema de IA español a través de un organismo de inspección que vigile la actividad de las empresas que lo incorporen a sus equipos fabricados.

Artículo 30. Financiación e incentivos fiscales.

1. Las Administraciones Públicas, en el ámbito de sus competencias, desarrollarán las siguientes actuaciones:

a) Promover medios de financiación pública para estimular y atraer las inversiones privadas en el entorno de la IA *y Big Data.*
b) Diseñar un plan coordinado entre la inversión pública y la privada para estas tecnologías.
c) Dotar de recursos suficientes y adecuados los programas de becas y subvenciones a los sectores de la IA *y Big Data.*

cve: BOCG-14-B-173-1

2. Las empresas tecnológicas digitales, en especial las que utilicen sistemas basados en Inteligencia Artificial se incluirán en la regulación del artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades referente a la deducción por actividades de investigación y desarrollo e innovación tecnológica.

Artículo 31. Consumidores de sistemas basados en IA.

1. Los consumidores recibirán información clara sobre la utilización, características y propiedades de los productos que utilizan Inteligencia Artificial.
2. Los usuarios podrán contar con las herramientas necesarias para controlar los datos generados y distinguir si se están comunicando con un sistema o con un usuario. En particular, cuando se esté interactuando con un sistema automatizado, se deberá conocer el carácter de esta interactuación, conociendo en qué momento es más conveniente ponerse en contacto con una persona, así como la forma de garantizar que las decisiones del sistema puedan verificarse o corregirse.

Artículo 32. Reconocimiento biométrico.

1. Se permitirá el uso del reconocimiento facial y biométrico basado en IA para fines de identificación personal, siempre que se respete la legislación actual.
2. Se regulará el uso generalizado de esta tecnología para la vigilancia, rastreo o evaluación, basados en clasificación del comportamiento o emociones de las personas.
3. En materia de ética, las autoridades públicas garantizarán que los marcos reglamentarios para el desarrollo y el uso de las tecnologías de IA estén en consonancia con los valores y derechos fundamentales.

Artículo 33. Derechos de propiedad intelectual derivados del uso de IA.

Respecto a los derechos de propiedad intelectual y patentes, la persona física o jurídica que inicie el proceso de creación, con independencia del autor del algoritmo utilizado por el sistema, será considerado el autor de las obras generadas con IA.

CAPÍTULO III

Aeronaves no tripuladas. Drones

Artículo 34. Aeronaves no tripuladas.

Las Administraciones Públicas, en el ámbito de sus competencias, impulsarán la creación de un marco europeo del uso de aeronaves no tripuladas o drones, dirigido al ámbito de operaciones de búsqueda, salvamento y contraincendios, bien sean autónomos o por control remoto, y que no estén contemplados específicamente en el Reglamento de Ejecución (UE) 2019/947 de la Comisión de 24 de mayo de 2019 relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas.

Artículo 35. Empleo de drones civiles en el sector comercial e industrial.

1. La Agencia Estatal de Seguridad Aérea (AESA) elaborará, en el plazo de doce meses desde la entrada en vigor de la presente ley, el Plan Nacional de Aerovías y Rutas españolas para la navegación ordenada de aeronaves no tripuladas pilotadas por control remoto o autónomas, estableciendo una red de corredores aéreos que permitan su empleo para uso comercial, industrial y, en particular, para el transporte. El Plan Nacional de Aerovías y Rutas será elevado al Consejo de Ministros para su aprobación.
2. El Plan Nacional de Aerovías y Rutas establecerá espacios aéreos segregados o aerovías exclusivas para UAS civiles de uso comercial e industrial, especialmente de transporte.
3. En el plazo de doce meses desde la entrada en vigor de la presente ley, el ministerio que tenga entre sus competencias el transporte y la aviación civil, previo informe preceptivo de la Agencia Estatal de Seguridad Aérea, revisará la normativa reglamentaria en materia de aeronaves no tripuladas, pilotadas por control remoto o autónomas, con la finalidad de establecer un procedimiento de autorización simplificado para la utilización del espacio aéreo con fines comerciales o industriales.

cve: BOCG-14-B-173-1

4. Este marco legal se elaborará conforme a los requisitos establecidos en el Reglamento de Ejecución (UE) 2019/947.

Artículo 36. Empleo de drones civiles en usos de última milla.

1. El Ministerio que tenga entres sus funciones el transporte y la aviación civil, previo informe preceptivo de la AESA, realizará las siguientes actuaciones, conforme al Reglamento UE 2019/947 anteriormente citado, para el empleo de aeronaves no tripuladas en operaciones industriales o comerciales en usos de última milla:

a) Favorecer el establecimiento de bases y espacios específicos para el repostaje y mantenimiento de aeronaves no tripuladas en áreas logísticas, a fin de facilitar el cambio modal de las mercancías.
b) Establecer zonas en núcleos urbanos para la navegación aérea de aeronaves no tripuladas, en condiciones de seguridad y compatible con los usos urbanos.
c) Dictar medidas básicas para habilitar el entorno urbano a la navegación aérea de aeronaves civiles pilotadas por control remoto o autónomas, estableciendo las limitaciones correspondientes para la realización de usos de última milla.

2. Las Administraciones Públicas, en el ámbito de sus competencias, establecerán un sello de homologación nacional de drones que, junto con el marcado de CE (Comunidad Europea), garantice la seguridad de su fabricación ante posibles fallos y accidentes.

Artículo 37. Empleo de drones en el servicio postal universal.

El ministerio que tenga entres sus funciones el transporte y aviación civil, en coordinación con la Sociedad Estatal Correos y Telégrafos, impulsará la implantación de aeronaves no tripuladas pilotadas por control remoto en el desarrollo del servicio postal universal para las actividades de recogida, admisión, clasificación, transporte, distribución y entrega de envíos postales nacionales y transfronterizos, tanto de cartas y tarjetas postales, con las limitaciones de peso y tamaño impuestas por el Reglamento de Ejecución UE 2019/947, anteriormente citado, y el Reglamento Delegado 2019/945 de la Comisión, de 12 de marzo de 2019, sobre los sistemas de aeronaves no tripuladas y los operadores de terceros países de sistemas de aeronaves no tripuladas.

Artículo 38. Empleo de drones para el transporte de mercancías.

1. Se autoriza el uso de aeronaves civiles pilotadas por control remoto para el transporte de medicamentos, baterías, balizas o equipamiento médico, en situaciones de emergencia.
2. En el ámbito civil, podrán utilizarse drones para el reparto en zonas de difícil acceso para mejorar la accesibilidad de todos los territorios y ciudadanos españoles y reducir el impacto medioambiental producido por el sector del transporte.

Artículo 39. Normativa municipal.

1. Las Ordenanzas Municipales de uso de aeronaves civiles pilotadas por control remoto o autónomas, serán acordes con otras ordenanzas municipales en materia de seguridad y convivencia ciudadana.
2. Se permitirá a los ayuntamientos, en el ámbito de sus competencias, el uso de drones en situaciones de grave riesgo, emergencia o catástrofe pública, así como para la protección y socorro de personas y bienes, o cuando les sea requerido por las autoridades responsables de la gestión de dichas situaciones.
3. Se permitirá a los ayuntamientos el uso de drones para la mejora de las funciones propias de la policía municipal, tales como proteger el libre ejercicio de los derechos y libertades de los ciudadanos, garantizando su seguridad; vigilar y realizar informes sobre daños y anomalías en las vías públicas, parques, jardines o lugares y bienes que constituyen el patrimonio municipal; denunciar las obras y actividades ilícitas sometidas a la ordenación y disciplina del Ayuntamiento; vigilar y ordenar el tráfico, controlando la circulación y el estacionamiento de vehículos; vigilar la salubridad e higiene de zonas públicas; y cualquier otra función contemplada en sus ordenanzas municipales.

cve: BOCG-14-B-173-1

4. Los ayuntamientos, en el uso de sus competencias, aplicarán los requisitos establecidos en el citado Reglamento de Ejecución (UE) 2019/947 por parte de los operadores y pilotos de drones, ya sean recreativos o profesionales, estableciendo las sanciones correspondientes.

5. Los ayuntamientos, en el ámbito de sus competencias, establecerán ordenanzas municipales para fomentar e incentivar el desarrollo y el uso de drones para uso comercial y entrega de paquetería.

Artículo 40. Incentivos fiscales en la tecnología de drones.

Las empresas tecnológicas digitales, incluidas las que utilicen aeronaves civiles pilotadas por control remoto, se incluirán en la regulación del artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades referente a la deducción por actividades de investigación y desarrollo e innovación tecnológica.

Artículo 41. Impacto ambiental.

1. Las aeronaves no tripuladas, bien sean pilotadas por control remoto o autónomas, y que se utilicen para usos comerciales e industriales deberán respetar los espacios naturales y evitar la alteración del comportamiento animal.

2. Los responsables del uso de drones serán responsables del cumplimiento de la normativa medioambiental y, en particular, del Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y por el que se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea.

CAPÍTULO IV

Vehículo conectado y parcialmente automatizado

Artículo 42. Protección de datos.

1. Los vehículos conectados y parcialmente automatizados están sujetos al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que se aplica cuando el procesamiento de datos en el contexto de vehículos conectados implique el procesamiento de datos personales de individuos.

2. Los usuarios de un vehículo conectado están protegidos por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. Las Administraciones Públicas, en el ámbito de sus competencias, promoverán el despliegue de una infraestructura de comunicaciones dedicada a vehículos conectados en las distintas carreteras.

Artículo 43. Protección de los vehículos frente a ciberataques.

1. Los fabricantes y suministradores de componentes de vehículos conectados estarán obligados a cumplir con las normas de certificación aprobadas por la UE, con especial atención a la norma WP29/2020/79 de Naciones Unidas.

2. Las Administraciones Públicas, en el ámbito de sus competencias, establecerán las siguientes actuaciones:

a) Promover campañas de difusión y concienciación ciudadana relativas a las ventajas para los pasajeros, peatones y ciclistas, de la incorporación de los nuevos servicios basados en Sistemas Avanzados de Asistencia a la Conducción (ADAS) y de intercambio de información en vehículos.

b) Elaborar normas claras e inequívocas para proteger la seguridad del usuario de vehículos conectados.

cve: BOCG-14-B-173-1

c) Establecer programas de apoyo para facilitar a fabricantes y suministradores de componentes la adaptación urgente de sus procesos de diseño y fabricación al cumplimiento de las normas de certificación aprobadas por la UE.

d) Establecer programas de difusión, información y apoyo a los talleres de vehículos y su personal, para adaptarlos a la nueva realidad tecnológica de los vehículos conectados y parcialmente automatizados.

e) Diseñar un plan de rediseño de los requisitos para la Inspección Técnica de Vehículos, así como de apoyo a la reconversión de las estaciones de inspección, para adaptarlas a la nueva realidad tecnológica de los vehículos conectados y parcialmente automatizados.

CAPÍTULO V

Internet de las Cosas (IoT)

Artículo 44. Fabricantes de sistemas IoT.

1. Se considera dispositivo conectado cualquier dispositivo u objeto físico que sea capaz de conectarse a Internet u otra red de datos, ya sea de manera directa o indirecta, y al que se le asigna a una dirección de protocolo de internet, a una dirección *Bluetooth* o cualquier otro acceso a tecnología inalámbrica o satelital.

2. El fabricante de dispositivos conectados tendrá la obligación de informar al consumidor de los riesgos, usos, posibles manipulaciones, defectos y, en especial, todo lo relacionado con su privacidad y confidencialidad.

3. Los fabricantes equipararán sus dispositivos con características de seguridad razonables y adecuadas a la naturaleza del mismo y a la información que recopila.

4. Los fabricantes diseñarán dispositivos conectados con indicadores visuales, auditivos u otros que alerten a los consumidores cuando estén transmitiendo información personal.

Artículo 45. Seguridad en sistemas IoT.

1. En el caso de que los dispositivos conectados a Internet tengan contraseñas por defecto, éstas serán sólidas y seguras. Además, en sus instrucciones, figurará de forma expresa y visible la importancia de establecer, desde el comienzo de su utilización, contraseñas seguras para evitar los ciberataques.

2. Las Administraciones, en el marco de sus competencias, establecerán las siguientes medidas para la seguridad de los sistemas de IoT:

a) Salvaguardar la seguridad y la privacidad, tanto de los consumidores como de las empresas, en el ámbito IoT.

b) Adoptar medidas para la inspección, seguimiento y control de la fabricación de los dispositivos conectados.

c) Delimitar la responsabilidad de los profesionales en la cadena de suministro del producto.

d) Establecer mecanismos de participación de las empresas que fabriquen dispositivos conectados para la solución de controversias y la adaptación de nuevas tecnologías aplicadas a IoT.

CAPÍTULO VI

Computación en la nube

Artículo 46. Limitación de responsabilidad.

Las organizaciones que contraten servicios de nube pública, establecerán límites de responsabilidad compartida entre los proveedores de servicios de nube y los contratantes y evitarán poner en riesgo información sensible de empleados, clientes, proveedores y todos los que participen en el flujo del negocio.

Artículo 47. Incentivos para empresas de infraestructuras Cloud.

1. Las empresas proveedoras de servicios *Cloud,* con sistemas hardware físicos ubicados en el territorio nacional, se incluirán como sector de actividad para optar a la categoría de consumidor

cve: BOCG-14-B-173-1

electrointensivo y se beneficiarán, por tanto, de los mecanismos de ayuda para esta figura de consumidor que contempla el Estatuto del Consumidor electrointensivo.

2. Las Administraciones Públicas, en el ámbito de sus competencias:

a) Establecerán programas de apoyo para la implantación, en el territorio nacional, de los sistemas *hardware* físicos de los proveedores de la nube.

b) Promoverán la colaboración público-privada para la capacitación y formación digital de profesionales en las administraciones públicas y sector privado para la gestión de servicios *Cloud.*

c) Establecerán programas de incentivos para la migración y el acceso de nuevos servicios *Cloud* para PYME y autónomos.

CAPÍTULO VII

Blockchain

Artículo 48. Criptomonedas.

1. Las criptomonedas podrán ser aceptadas en el cumplimiento de obligaciones privadas, en la medida en que sean libremente concertadas por las partes en la transacción como métodos alternativos, contractuales e inmediatos de pago y se usen sin ningún otro propósito que el de servir como tales, sin perjuicio de la normativa sobre medios de pago y curso legal aplicable.

2. Las obligaciones privadas que impliquen intercambio de bienes o servicios con criptomonedas estarán sujetas al mismo régimen fiscal que las transacciones monetarias. Todo ello se entiende sin perjuicio de la sujeción a impuestos que corresponda a las entidades emisoras de criptomonedas, los proveedores de servicio de cambio de moneda virtuales por monedas fiduciarias y prestadores de servicios de claves o monederos virtuales.

3. Se considerarán entidades sujetas a la regulación de blanqueo de capitales, a los proveedores de servicios de cambio de moneda virtual por monedas fiduciarias y a los prestadores de servicios de custodia, quedando obligadas a la identificación de sus clientes. En ningún caso, el uso de criptomonedas eximirá del cumplimiento de las normas sobre blanqueo de capitales y la legislación aplicable a la operación que se realice con intercambio de las mismas.

4. Las Administraciones Públicas, en el marco de sus competencias, aplicarán los controles pertinentes para las operaciones de compraventa o *trading* de criptomonedas con el fin de que se cumplan las obligaciones fiscales correspondientes.

5. Las Administraciones Públicas, en el ámbito de sus competencias, enviarán requerimientos de información a las entidades financieras, casas de cambio, pasarelas de pago y entidades vinculadas con cajeros automáticos que intervienen en la adquisición o venta de criptomonedas, así como a las empresas que admiten pagos con criptomonedas.

6. Los ciudadanos que utilicen criptomonedas para operaciones financieras tendrán el derecho a la seguridad de sus datos y a obtener información de las mismas, mediante servidores privados y registros *Blockchain,* y estarán protegidos por la legislación vigente relativa a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Artículo 49. Oferta inicial de moneda (ICO).

1. Las criptomonedas y los llamados *tokens* que se emiten al lanzar una Oferta Inicial de Monedas (ICO), quedarán comprendidos en el concepto de valor negociable, según el artículo 2.1 del Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores y, por tanto, se someterán a las exigencias de la misma, siempre que cumplan los requisitos legalmente establecidos. En todo caso, la consideración de valor negociable estará sujeta a las determinaciones de la Comisión Nacional del Mercado de Valores.

2. Lo establecido en el apartado anterior será de aplicación, no sólo a los *tokens* que atribuyan algún derecho o expectativa de beneficio asociado a un negocio, sino también a aquellos otros que faciliten el acceso a un servicio o la compra de productos, siempre que exista esa expectativa de revalorización del valor.

cve: BOCG-14-B-173-1

3. Las Administraciones Públicas, en el marco de sus competencias, aplicarán los controles pertinentes sobre el dinero que se recaude en las ICO, con el fin de que éstas cumplan con las obligaciones fiscales correspondientes.

4. El inversor de una ICO no tendrá el deber de informar a las autoridades pertinentes sobre una inversión que realice por debajo de los 6.000 euros.

Artículo 50. Consejo Nacional de Criptoactivos.

1. Se crea el Consejo Nacional de Criptoactivos (CNC) como entidad administrativa del sector público con fines consultivos, formado por representantes de la Dirección General del Tesoro, la Comisión Nacional del Mercado de Valores y del Banco de España, dependiente del Ministerio de Hacienda, a través de la Agencia Estatal de la Administración Tributaria.

2. El Consejo Nacional de Criptoactivos tendrá entre sus funciones:

a) Estudiar y analizar las implicaciones del uso de los criptoactivos y otras formas de bienes y servicios que utilizan la tecnología *Blockchain.*

b) Evaluar la introducción de *Blockchain* en el sector público español con el objetivo de mejorar los procesos internos, aportar trazabilidad, robustez y transparencia en la toma de decisiones y ofrecer recomendaciones.

c) Velar por el establecimiento de mecanismos para detectar el fraude, la evasión de capitales y el terrorismo.

3. El Reglamento del Consejo Nacional será aprobado por el Consejo de Ministros en el plazo de seis meses desde la entrada en vigor de la presente ley.

4. Este órgano elaborará un Libro de Criptoderecho, que se actualizará mediante adendas de la Comisión Nacional del Mercado de Valores, al menos anualmente, con las recomendaciones para garantizar las buenas prácticas y buen uso en el marco del intercambio *Blockchain* y el uso de criptomonedas en actividades de las entidades financieras o de aquellas otras que, de alguna manera, participen o estén presentes profesionalmente en los mercados financieros. Dichas recomendaciones se basarán en los principios de transparencia en la cadena de bloques de las transacciones, irrevocabilidad e integridad de los datos, así como la inmutabilidad de su contenido en cada bloque.

5. El Libro de Criptoderecho gozará de plena publicidad y se fomentará su difusión y conocimiento.

Artículo 51. Hipotecas, seguros e indemnizaciones.

1. En el sistema hipotecario, los propietarios podrán utilizar una criptomoneda propia a través de la cual pagar su hipoteca.

2. El sector inmobiliario podrá utilizar una criptomoneda propia para invertir en grupos de hipotecas.

3. Los bancos podrán utilizar *Blockchain* como sistema para gestionar hipotecas y seguros y agilizar el pago de indemnizaciones con divisas electrónicas.

4. En las pólizas de seguros, podrán utilizarse contratos inteligentes que conformen unas condiciones en función de los trámites a seguir, los procesos de verificación, gestión y adecuación de las pólizas a los potenciales incidentes.

Artículo 52. Régimen jurídico general de la tecnología Blockchain.

1. Los contratos inteligentes *(Smart Contracts)* se regirán por lo establecido en el artículo 23 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico y por el régimen jurídico general que se contempla en el Código Civil.

2. Los productos alimentarios podrán contar con un pasaporte en el que se asigne una etiqueta asociada a cada producto con información codificada en una cadena de bloques personal, intransferible e inalterable, para que quede constancia de su paradero y se utilizará el sistema *Blockchain* para su trazabilidad de principio a fin.

3. Los centros sanitarios podrán usar la tecnología *Blockchain* con el fin de ofrecer una mayor trazabilidad en las decisiones y procesos médico-hospitalarios, así como en las gestiones de equipos valiosos de hospitales o expedientes médicos que impliquen decisiones de diferentes especialistas. En esos casos, el paciente será el propietario de su historial digital y decidirá a quién permite el acceso.

cve: BOCG-14-B-173-1

4. Las Administraciones Públicas, en el ámbito de sus competencias, impulsarán medidas para garantizar la autenticad de medicamentos, mediante el establecimiento de tecnología *Blockchain* en los centros farmacéuticos que registre y garantice el seguimiento, desde que el fármaco se crea en el laboratorio hasta que llega al consumidor final.

5. Las Administraciones Públicas, en el ámbito de sus competencias, fomentarán la implantación de plataformas digitales, tecnología *blockchain,* contratos inteligentes y otras formas de automatización para la transparencia, simplificación, seguridad y trazabilidad en el comercio.

6. Las Administraciones Públicas, en el ámbito de sus competencias, impulsarán un marco de identidad digital distribuida basada en Blockchain para personas físicas y jurídicas.

Artículo 53. Operaciones fraudulentas de blanqueo de capitales y terrorismo.

1. Las Administraciones Públicas, en el ámbito de sus competencias, utilizarán *Blockchain* para garantizar la transparencia en las operaciones con criptomonedas y evitar el blanqueo y la fuga de capitales.

2. A tal fin, se dotará de recursos y formación adecuada y suficiente a los Cuerpos de la Administración del Estado que tengan entre sus funciones detectar y evitar casos de fraude, estafas y ataques de *hackers* relacionados con las ICO, la creación, control y mantenimiento de un registro de proveedores *exchanges* y proveedores de servicios de custodia de monederos electrónicos, evitando así el anonimato y la financiación de operaciones fraudulentas y terroristas.

Artículo 54. Protección del medio ambiente.

1. Las empresas que utilicen *Blockchain,* deberán establecer planes para impulsar la investigación del diseño de nuevas herramientas de gestión del consumo para la mejora de la eficiencia energética en España.

2. Las empresas emitirán un certificado de trazabilidad de energías limpias o renovables cuando se inyecte energía a la red.

3. Las Administraciones Públicas, en el ámbito de sus competencias, elaborarán las directrices para la emisión del certificado establecido en el apartado anterior.

Artículo 55. Protección de usuarios.

1. Los ciudadanos que utilicen criptomonedas para operaciones financieras tienen el derecho a la seguridad de sus datos y a obtener información de las mismas mediante servidores privados y registros Blockchain. Además, estarán protegidos por la legislación vigente relativa a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. En el ámbito de los procesos judiciales y arbitrales, se admitirá la tecnología *Blockchain* como fuerza probatoria de los documentos privados.

Artículo 56. Fiscalidad.

1. Las empresas tecnológicas digitales, en especial las que utilicen la tecnología *Blockchain* y las criptomonedas, se incluirán en la regulación del artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades referente a la deducción por actividades de investigación y desarrollo e innovación tecnológica. La deducción de los gastos efectuados en el período impositivo será de cinco puntos más de lo establecido en el punto c) del citado artículo, durante dos años.

2. Las Administraciones Públicas, en el ejercicio de sus funciones, enviarán requerimientos de información a las entidades financieras, casas de cambio, pasarelas de pago y entidades vinculadas con cajeros automáticos que intervienen en la adquisición o venta de criptomonedas, así como a las empresas que admiten pagos por este medio.

cve: BOCG-14-B-173-1

TÍTULO QUINTO

Protección digital ciudadana

CAPÍTULO I

Derechos digitales y obsolescencia programada

Artículo 57. Derechos digitales.

1. Los derechos y libertades establecidos en la Constitución, así como en los tratados y convenios internacionales en los que España forme parte, son de aplicación a las actuaciones de las personas en Internet.

2. Se consideran derechos digitales a los establecidos en los artículos del 79 al 90 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. Las Administraciones Públicas, en el ámbito de sus competencias, garantizarán los derechos digitales de los ciudadanos estableciendo las siguientes medidas:

a) Garantizar el acceso a Internet de todos los ciudadanos españoles, así como promover medidas para eliminar la brecha digital.

b) Ampliar las competencias de la Oficina de Atención al Usuario de Telecomunicaciones para dar cobertura a todos los usuarios consumidores de servicios digitales a nivel estatal.

c) Establecer, para todos los servicios digitales, la posibilidad de identificarse de manera segura, siguiendo el esquema de la autenticación reforzada o *Strong Customer Authentication* (SCA), establecida por la Directiva Europea 2015/2366 sobre servicios de pago en el mercado interior conocida como PSD2, con el objetivo de reforzar la seguridad en las compras online.

4. Las empresas tendrán la obligación de disponer de herramientas digitales para que los usuarios puedan reclamar el respeto a sus derechos. Para ello, las empresas prestadoras de los servicios digitales a ciudadanos españoles, independientemente de su lugar de establecimiento o ubicación física, seguirán las directrices del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Así mismo, estos servicios se someterán a las mismas normas de protección de derechos de usuarios que los servicios de comunicaciones electrónicas y contarán con los mismos mecanismos alternativos de resolución de conflictos que dichos servicios.

5. Las Administraciones Públicas, en el ámbito de sus competencias, garantizarán que los riesgos de comisión de delitos en el ámbito de sus servicios dirigidos a ciudadanos españoles se gestionen de forma adecuada y que las autoridades competentes dispongan de las herramientas necesarias para garantizar la persecución de delitos en el ámbito digital.

6. El lugar de establecimiento de la empresa prestadora no podrá suponer la inexistencia de pagos monetarios a cambio de acceso a datos del consumidor o usuario.

Artículo 58. Obsolescencia programada.

1. La obsolescencia programada es la determinación del fin de la vida útil de productos tecnológicos fabricados para el consumo particular que, tras un período de tiempo calculado previamente por el fabricante, se vuelven obsoletos e inservibles por falta de repuestos o dificultad de reparación.

2. Las Administraciones Públicas protegerán los derechos de los consumidores y usuarios cuando la obsolescencia programada afecte directamente a bienes o servicios de uso o consumo común, ordinario y generalizado.

3. A los actos derivados de la obsolescencia programada se aplicará lo establecido en los artículos 5, 6 y 7 de la Ley 3/1991, de 10 de enero, de Competencia Desleal sobre actos de engaño, confusión u omisión engañosa.

cve: BOCG-14-B-173-1

4. Las Administraciones Públicas, en el ámbito de sus competencias, realizarán las siguientes acciones:

a) Establecer el tiempo que deben estar disponibles para los consumidores las piezas de recambio de los productos tecnológicos, fabricados para el consumo.
b) Crear un Órgano de Inspección específico, dependiente del Ministerio que tenga entre sus competencias las de Industria, para detectar casos de obsolescencia programada.

CAPÍTULO II

Seguridad digital

Artículo 59. Protección del menor.

El Ministerio que tenga entre sus competencias la Protección del Menor, impulsará las siguientes acciones:

1. Velar por el cumplimiento de lo establecido en los artículos 7, 84 y 92 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sobre la protección del menor en Internet.
2. Diseñar campañas de divulgación en los medios de comunicación sobre el uso adecuado de las redes sociales, los peligros de la difusión de imágenes personales, la protección de datos y el uso de IoT por los menores.
3. Fomentar actividades de formación dirigida a familias, profesorado y alumnado para garantizar el honor y la intimidad personal de los menores en los centros escolares y protegerlos del ciberacoso y de la adicción a la tecnología.
4. Dotar a los centros escolares de herramientas para tener una presencia segura en Internet y conocer los mecanismos necesarios de actuación cuando sea necesario.
5. Coordinar las acciones divulgativas y formativas realizadas por otros Ministerios y Organismos oficiales dirigidas a los centros escolares como el Defensor del Menor, el Instituto Nacional de Ciberseguridad (INCIBE), la Agencia Española de Protección de Datos (AEPD) o el Ministerio de Educación.

Artículo 60. Reserva Estratégica en Ciberseguridad.

1. El Ministerio de Defensa creará un cuerpo de Reserva Estratégica de Talento en Ciberseguridad.
2. Serán reservistas voluntarios pertenecientes a la Reserva Estratégica de Talento en Ciberseguridad los españoles que, en aplicación del derecho y deber constitucionales de defender a España y, habiendo solicitado participar en la correspondiente convocatoria, resulten seleccionados para desempeñar las funciones que se les encomienden bajo la dirección de las autoridades competentes del Ministerio de Defensa, para los cometidos específicos de carácter civil o militar que se señalen. Estos ciudadanos se vincularán de forma temporal y voluntaria con las Fuerzas Armadas por medio de un compromiso de disponibilidad.
3. Para formar parte de esta reserva específica, el Estado Mayor de la Defensa (EMAD) mediante el Mando Conjunto de Ciberdefensa (MCCD) seleccionará a aquellas personas que, por su experiencia y conocimientos técnicos o de otra índole en la materia, puedan aportar talento a las capacidades existentes en las Fuerzas Armadas. La Reserva Estratégica de Talento en Ciberseguridad, dependerá orgánicamente del EMAD a través del MCCD.
4. Las condiciones para optar a las plazas de ingreso en la Reserva Estratégica de Talento en Ciberseguridad que se convoquen, serán las siguientes:

a) Tener la nacionalidad española, tener cumplidos dieciocho años y que acredite las titulaciones y cumplir las especificaciones que, reglamentariamente, se determinen, así como el cumplimiento de los requisitos generales de ingreso actualmente requeridos.
b) Para adquirir la condición de reservista voluntario habrá que obtener una de las plazas ofertadas en convocatoria pública, organizada por el Estado Mayor de la Defensa, y superar los periodos de formación, básica y específica. El proceso de selección subsiguiente deberá garantizar, en todo caso, los

cve: BOCG-14-B-173-1

principios constitucionales de igualdad, mérito y capacidad, así como los demás principios rectores para el acceso al empleo público, siempre teniendo en cuenta la necesaria garantía de la protección de la integridad y confidencialidad de la información y los sistemas.

c) La condición de reservista voluntario se considerará actividad exceptuada del régimen de incompatibilidades del personal al servicio de las Administraciones Públicas.

5. Los reservistas de la Reserva Estratégica de Talento en Ciberseguridad firmarán un compromiso inicial de cuatro años. Posteriormente podrán firmar nuevos compromisos, de conformidad con el procedimiento que reglamentariamente se establezca, por períodos de tres años.

6. Respecto a los derechos de los reservistas voluntarios de la Reserva Estratégica de Talento en Ciberseguridad:

a) Tendrán, inicialmente, los empleos de alférez (RV) o alférez de fragata (RV), sargento (RV) y soldado (RV) o marinero (RV), según la categoría a la que hayan accedido en la correspondiente convocatoria. Reglamentariamente, se determinará la forma de ascender a empleos superiores, estableciendo sus atribuciones y los procedimientos, requisitos y condiciones, especialmente las referidas a los tiempos mínimos en que deberán haber permanecido activados.

b) El reservista, al objeto de su identificación se les facilitará la correspondiente tarjeta de identidad militar para personal reservista.

c) Finalizado el compromiso adquirido, cesará en la condición de reservista, recibiendo el título de oficial de reservista honorífico, así como las distinciones que se establezcan por el Ministro de Defensa en función de la duración de los compromisos y servicios prestados.

7. Los reservistas voluntarios cibernéticos pasarán a desarrollar sus funciones al servicio de las Fuerzas Armadas cuando sean activados. No obstante, y por las especiales características de su actividad, estarán en situación de disponibilidad durante todo el período que dure su compromiso. Ello supone que, cuando sea necesario, les podrán ser encomendados cometidos de apoyo a las tareas de ciberseguridad sin necesidad de su incorporación a su unidad de activación en caso de que las circunstancias que concurran así lo hagan necesario.

8. Los periodos de desarrollo de funciones militares por parte de los reservistas tendrán la consideración de permisos retribuidos, previo acuerdo con la empresa.

9. En el caso de que los reservistas fueran funcionarios al servicio de las Administraciones Públicas, los períodos de desempeño de funciones encomendadas por el EMAD serán considerados como permiso regulado en el artículo 48 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.

Disposición adicional primera.

1. Se adiciona un último párrafo al apartado 1 a) del artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, que queda redactado de la siguiente manera: «Además, se considerará actividad de investigación y desarrollo las empresas tecnológicas digitales, en especial las que utilicen la tecnología *Blockchain* y las criptomonedas y cualquier otra que surja de su desarrollo y evolución».

2. Se adiciona un último párrafo en el apartado 2a) del artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, que queda redactado de la siguiente manera: «Además, se considerará innovación tecnológica las actividades derivadas del uso de *Blockchain* y las criptomonedas y cualquier otra que surja de su desarrollo y evolución».

3. Se adiciona el apartado 2 b) 5.º del artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, que queda redactado de la siguiente manera: «Actividades de tecnología digital, especialmente las basadas en el uso de *Blockchain* y las criptomonedas».

Disposición adicional segunda.

Se adiciona un último párrafo al apartado 2 del artículo 326 Fuerza probatoria de los documentos privados, de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil que queda redactado como sigue: «Se admite como medio de prueba de autenticidad la información incluida en un documento validado por el sistema *Blockchain*».

cve: BOCG-14-B-173-1

Disposición adicional tercera.

Se adiciona un apartado g) al artículo 8 sobre Derechos básicos de los consumidores y usuarios, del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementaria, que queda redactado de la siguiente manera: «g) La protección contra los riesgos que puedan afectar su salud o seguridad respecto a los productos o servicios basados en sistemas de Inteligencia Artificial, algoritmos y robots».

Disposición adicional cuarta.

Se adiciona un apartado 4 en el artículo 122 de la Ley 39/2007, de 19 de noviembre, de la carrera militar, que queda redactado como sigue:

«4. También son reservistas los correspondientes a la Reserva Estratégica de Talento en Ciberseguridad, en los términos que legal y reglamentariamente se determine.»

Disposición derogatoria primera.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan, contradigan o resulten incompatibles con lo dispuesto en la presente ley.

Disposición final primera. Habilitación para el desarrollo reglamentario.

Se autoriza al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y aplicación de lo establecido en esta ley, así como acordar las medidas para garantizar la efectiva ejecución e implantación de las previsiones de esta ley.

Disposición final segunda. Títulos Competenciales.

Esta ley se dicta al amparo de la competencia exclusiva que atribuye al Estado el artículo 27 de la Constitución Española que atribuye al Estado la competencia en materia de Educación; el artículo 39 sobre la protección a la familia y a la infancia; el artículo 45 referido a la protección del medio ambiente; el artículo 51 en materia de defensa de los consumidores y usuarios; el artículo 130 respecto a la modernización y desarrollo de todos los sectores económicos y el tratamiento especial a las zonas de montaña; el artículo 149.1.4.º sobre Defensa y Fuerzas Armadas; el artículo 149.1.5.º en materia de Justicia; el 149.1.6.º en materia de legislación penal; el artículo 149.1.7.º sobre legislación laboral; el artículo 149.1.13.º en materia de bases y coordinación de la planificación general de la actividad económica; el artículo 149.1.14.º sobre Hacienda general y Deuda del Estado; el 149.1.15.º en materia de y coordinación general de la investigación científica y técnica; el artículo 149.1.18.º que atribuye al Estado la competencia para dictar las bases del régimen jurídico de las Administraciones Públicas y competencia en materia de procedimiento administrativo común y sistema de responsabilidad de todas las Administraciones Públicas; el artículo 149.1.20.º en materia Marina mercante y abanderamiento de buques; iluminación de costas y señales marítimas; puertos de interés general; aeropuertos de interés general; control del espacio aéreo, tránsito y transporte aéreo, servicio meteorológico y matriculación de aeronaves; el artículo 149.1.23.º en materia de protección del medio ambiente; y 149.1.30.º en materia de obtención, expedición y homologación de títulos académicos y profesionales; y el artículo 149.2 referente al servicio de la cultura como deber.

Disposición final tercera. Entrada en vigor.

Esta ley entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado», excepto las medidas que impliquen un aumento de los créditos o una disminución de los ingresos en relación con el presupuesto vigente, que no entrarán en vigor, en la parte que comporte afectación presupuestaria, hasta el ejercicio presupuestario siguiente al de la entrada en vigor.

cve: BOCG-14-B-173-1